M336 Unit GR3
Mathematics and Computing
A third-level course

GROUPS & GEOMETRY

BLOCK THREE
UNIT GR3

Decomposition of Abelian groups

The Open University

M336

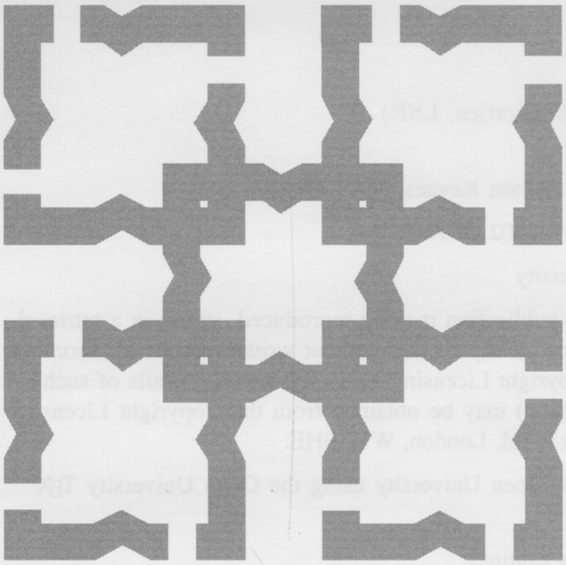
Mathematics and Computing: a third-level course

GROUPS & GEOMETRY

UNIT GR3 DECOMPOSITION OF ABELIAN GROUPS

Prepared for the course team by

Bob Coates & Bob Margolis



The Open University

This text forms part of an Open University third-level course.
The main printed materials for this course are as follows.

Block 1

Unit IB1	Tilings
Unit IB2	Groups: properties and examples
Unit IB3	Frieze patterns
Unit IB4	Groups: axioms and their consequences

Block 2

Unit GR1	Properties of the integers
Unit GR2	Abelian and cyclic groups
Unit GE1	Counting with groups
Unit GE2	Periodic and transitive tilings

Block 3

Unit GR3	Decomposition of Abelian groups
Unit GR4	Finite groups 1
Unit GE3	Two-dimensional lattices
Unit GE4	Wallpaper patterns

Block 4

Unit GR5	Sylow's theorems
Unit GR6	Finite groups 2
Unit GE5	Groups and solids in three dimensions
Unit GE6	Three-dimensional lattices and polyhedra

The course was produced by the following team:

Andrew Adamyk (BBC Producer)
David Asche (Author, Software and Video)
Jenny Chalmers (Publishing Editor)
Bob Coates (Author)
Sarah Crompton (Graphic Designer)
David Crowe (Author and Video)
Margaret Crowe (Course Manager)
Alison George (Graphic Artist)
Derek Goldrei (Groups Exercises and Assessment)
Fred Holroyd (Chair, Author, Video and Academic Editor)
Jack Koumi (BBC Producer)
Tim Lister (Geometry Exercises and Assessment)
Roger Lowry (Publishing Editor)
Bob Margolis (Author)
Roy Nelson (Author and Video)
Joe Rooney (Author and Video)
Peter Strain-Clark (Author and Video)
Pip Surgey (BBC Producer)

With valuable assistance from:

Maths Faculty Course Materials Production Unit
Christine Bestavachvili (Video Presenter)
Ian Brodie (Reader)
Andrew Brown (Reader)
Judith Daniels (Video Presenter)
Kathleen Gilmartin (Video Presenter)
Liz Scott (Reader)
Heidi Wilson (Reader)
Robin Wilson (Reader)

The external assessor was:

Norman Biggs (Professor of Mathematics, LSE)

The Open University, Walton Hall, Milton Keynes, MK7 6AA.

First published 1994. Reprinted 1997, 2002, 2007.

Edited, designed and typeset by the Open University using the Open University TEX System.

Printed in Malta by Gutenberg Press Limited.

ISBN 0 7492 2165 8

This text forms part of an Open University Third Level Course. If you would like a copy of *Studying with the Open University*, please write to the Central Enquiry Service, PO Box 200, The Open University, Walton Hall, Milton Keynes, MK7 6YZ. If you have not already enrolled on the Course and would like to buy this or other Open University material, please write to Open University Educational Enterprises Ltd, 12 Cofferidge Close, Stony Stratford, Milton Keynes MK11 1BY, United Kingdom.

1.3

MIX
Paper from responsible sources
FSC www.fsc.org
FSC® C022612

The paper used for this book is FSC-certified and totally chlorine-free. FSC (the Forest Stewardship Council) is an international network to promote responsible management of the world's forests.

CONTENTS

STUDY GUIDE

This unit builds on the material in *Unit GR2*, but also makes use of some of the ideas from *Units GR1* and *IB4* in particular.

Sections 2, 3 and 5 are of about average length, in terms of study time required. Section 1 is somewhat longer than average, but this is compensated for by Section 4 being rather short.

There is an audio programme associated with Section 3.

INTRODUCTION

In *Unit GR2* we expressed the Abelian groups of orders up to 8 in the form of direct products of cyclic groups as follows.

Order	Abelian group(s)
1	C_1
2	C_2
3	C_3
4	C_4, $C_2 \times C_2$
5	C_5
6	$C_6 \cong C_2 \times C_3$
7	C_7
8	C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$

In this unit we begin the task of showing that *every* finite Abelian group can be expressed as a direct product of cyclic groups in a way that is, essentially, unique.

Actually, we shall do a little more. We shall show that the same is true of any Abelian group generated by a finite number of its elements. We shall also show that, for *Abelian* groups, it *is* possible to decide whether two different specifications in terms of generators and relations define the same group, and we shall give an algorithm for doing so.

As we remarked in *Unit IB4*, it is *not* possible, *in general*, to decide whether or not two different specifications in terms of generators and relations define the same group.

Our work is based on the ideas about free groups that were discussed in *Unit IB4*.

In the first section we introduce the idea of a *free Abelian group* and use this to give a formal definition of what is meant by a *finitely presented Abelian group*. Informally, this means an Abelian group defined by a finite number of generators and a finite number of relations. The reason for this terminology is that a definition of a group in the form

$$G = \langle \text{a set of generators} : \text{ a set of relations} \rangle$$

is called a *finite presentation* of G.

We also show, in Section 1, how to associate with each such finite presentation a matrix with integer entries. For the simple case where the matrix is diagonal, we show that it is easy to identify the group as a direct product of cyclic groups.

In Section 2 we discuss an algorithm for reducing a non-diagonal matrix to a diagonal one which represents a new finite presentation for the original group.

Section 3 justifies why the method of reduction used in Section 2 must terminate and also must produce a diagonal matrix representing the same group.

Different applications of the reduction algorithm to a given finite presentation can lead to the group being represented in different ways as a direct product of cyclic groups. We also show in Section 3, by means of some examples, how it is possible to choose a unique standard, or *canonical*, direct product from the many possibilities.

The justification that the canonical form exists, and is unique, is given in Section 4. The proof makes use of the properties of direct products of cyclic groups of coprime orders.

Finally, the last section extends the decomposition of finitely presented Abelian groups to *finitely generated Abelian groups*.

1 FINITELY PRESENTED ABELIAN GROUPS

In this section we define what is meant by a free Abelian group and a finitely presented Abelian group.

In *Unit IB4*, we defined a free group on the generators

$$x_1, \ldots, x_n$$

to be the group whose elements are the reduced words in the symbols

$$x_1, \ldots, x_n, x_1^{-1}, \ldots, x_n^{-1}$$

with the operation of concatenation followed by reduction.

The term 'free' in the name means 'free of non-trivial relations' in the sense that the only relations between the group elements are those demanded by, or consequences of, the group axioms.

Any relation can be written in standard form as

$$w = e,$$

A relation in **standard form** is one whose right-hand side is simply e.

where w is a word in the free group and e is the identity (the empty word). Hence, in a free group, the only relation that can hold is where w reduces to the empty word by removing adjacent inverse pairs.

Also in *Unit IB4*, we defined what we meant by the group given by a set of generators and relations, that is a definition of the form

$$G = \langle a_1, \ldots, a_n : w_1 = e, \ldots, w_k = e \rangle$$

with generators

$$a_1, \ldots, a_n$$

and relations

$$w_1 = e, \ldots, w_k = e.$$

In fact G is defined as follows. We firstly take $\mathbb{F}_n$ as the free group generated by the n generators

$$x_1, \ldots, x_n.$$

Next we take the smallest normal subgroup K of $\mathbb{F}_n$ containing the reduced words in x_1 to x_n corresponding to the words w_1 to w_k. The group G is then defined to be the quotient group

$$G = \mathbb{F}_n / K.$$

To define an *Abelian* group in this manner, we ensure that the set of relations includes all expressions of the form

$$ab = ba, \quad \text{for all generators } a \text{ and } b$$

which becomes, in standard form,

$$aba^{-1}b^{-1} = e.$$

The alternative way of defining Abelian groups, which we adopt, is to start not with a free group but with a free Abelian group.

For the free group, the elements are reduced words in the generators and their inverses. In such words, the same generator could appear in *several* positions although not adjacent to its inverse. If we insist on the Abelian property, we can gather together *all* occurrences of each generator. We can then apply the usual rules of indices to express each element in the standard form

$$x_1^{s_1} \cdots x_n^{s_n}, \quad s_1, \ldots, s_n \in \mathbb{Z}.$$

We still require that there shall be no 'extra' relations, so the 'freeness' implies that

$$x_1^{s_1} \dots x_n^{s_n} = e$$

if and only if

$$s_1 = \dots = s_n = 0.$$

For Abelian groups we use, by and large, additive notation. So, a general element of the free Abelian group with generators

$$x_1, \dots, x_n$$

is

$$s_1 x_1 + \dots + s_n x_n, \quad s_1, \dots, s_n \in \mathbb{Z}.$$

The 'free' condition becomes

$$s_1 x_1 + \dots + s_n x_n = 0$$

if and only if

$$s_1 = \dots = s_n = 0.$$

This may well remind you of the definition of linear independence for vectors. The concepts are closely related.

Definition 1.1 Free Abelian group

The **free Abelian group** with generators

$$x_1, \dots, x_n$$

has elements

$$s_1 x_1 + \dots + s_n x_n, \quad s_1, \dots, s_n \in \mathbb{Z}.$$

The operation of addition is given by

$$(s_1 x_1 + \dots + s_n x_n) + (t_1 x_1 + \dots + t_n x_n)$$
$$= (s_1 + t_1) x_1 + \dots + (s_n + t_n) x_n.$$

Since addition in $\mathbb{Z}$ is commutative, this definition does indeed give an *Abelian* group.

Exercise 1.1

Show that, if

$$s_1 x_1 + \dots + s_n x_n = t_1 x_1 + \dots + t_n x_n$$

in the free Abelian group generated by

$$x_1, \dots, x_n,$$

then

$$s_1 = t_1, \dots, s_n = t_n.$$

The result of Exercise 1.1 shows that each element a of the free Abelian group has a *unique* expression of the form

$$a = s_1 x_1 + \dots + s_n x_n.$$

Hence a corresponds to a *unique* n-tuple of integers

$$(s_1, \dots, s_n)$$

which is an element of

$$\overbrace{\mathbb{Z} \times \dots \times \mathbb{Z}}^{n \text{ copies}}.$$

Conversely, each such n-tuple defines an element

$$a = s_1 x_1 + \dots + s_n x_n$$

of the free Abelian group with generators $x_1, \dots, x_n$.

Further, addition in the free Abelian group is carried out by adding corresponding coefficients, which corresponds exactly to element-wise addition in the direct product.
Hence, the function ϕ defined by

$$\phi((s_1, \ldots, s_n)) = s_1x_1 + \cdots + s_nx_n$$

is an isomorphism from the direct product of n copies of $\mathbb{Z}$ to the free Abelian group on the n generators $x_1, \ldots, x_n$.

This result can be summarized in the following theorem.

Theorem 1.1

The free Abelian group on the n generators

$$x_1, \ldots, x_n$$

is isomorphic to the direct product of n copies of $(\mathbb{Z}, +)$.

Further, the generators correspond to elements of the direct product as follows:

$$x_i \leftrightarrow (0, \ldots, 0, \overset{i\text{th place}}{1}, 0, \ldots, 0)\ .$$

The next step is to define precisely what we mean when we define an Abelian group in terms of generators and relations.

Notational convention

In future we shall use the following notational convention. Just as we have used G to denote a general group, we shall use A to denote a general *Abelian* group. Thus, if we make some statement about a group A, you should assume that A is Abelian even if this is not stated explicitly.

Thus, if we define A by

$$A = \langle a, b\colon\ 2a = 0,\ 3b = 0\rangle,$$

you should interpret this to mean that A is an Abelian group with the specified generators and relations, not a non-Abelian group that happens to have been written additively.

Example 1.1

What does it mean to define an Abelian group by writing

$$A = \langle a, b\colon\ 2a = 0,\ 3b = 0\rangle?$$

To define this group A, we proceed as for the non-Abelian case but use free Abelian groups instead of free groups.

Firstly, we take the free Abelian group F on the two generators x_1 and x_2, one for each generator of A.

Secondly, we find the smallest (normal) subgroup N of F containing the words corresponding to the relations

In an Abelian group all subgroups are normal.

$$2a = 0, \quad 3b = 0.$$

That is, N is the smallest subgroup of F containing the words $2x_1$ and $3x_2$.

Finally, we define the group A *to be* the quotient group

$$F/N.$$

So that defines the group A, but does not give a concrete model of it. However, we can obtain such a model for A by starting from the concrete model $\mathbb{Z} \times \mathbb{Z}$ for the free Abelian group F.

In this model $(1,0)$ corresponds to the generator x_1 of F and $(0,1)$ corresponds to x_2.

We ask you to establish that the subgroup K of $\mathbb{Z} \times \mathbb{Z}$ which corresponds to the subgroup N of F is given by

$$K = \{(2k, 3l) : \ k, l \in \mathbb{Z}\}. \qquad \diamond$$

Exercise 1.2

Write down the elements of $\mathbb{Z} \times \mathbb{Z}$ corresponding to the words $2x_1$ and $3x_2$ of F.

Exercise 1.3

Let K be the subgroup of $\mathbb{Z} \times \mathbb{Z}$ corresponding to the subgroup N of F. Prove that

$$K = \{(2k, 3l) : \ k, l \in \mathbb{Z}\}.$$

Example 1.1 continued

As a result of Exercise 1.3, instead of the quotient group F/N we can take the quotient group

$$(\mathbb{Z} \times \mathbb{Z})/K.$$

Every element of this quotient group is a coset of the form

$$(m, n) + K, \quad m, n \in \mathbb{Z}.$$

Since $(2,0) \in K$ we have

$$(2,0) + K = K.$$

Hence, every element of the quotient group is of the form

$$(0, n) + K \quad \text{or} \quad (1, n) + K.$$

Similarly, since $(0,3) \in K$, every element of the quotient group is of the form

$$(m, 0) + K, \quad (m, 1) + K \quad \text{or} \quad (m, 2) + K.$$

Combining these results gives the following six cosets

$$(0,0) + K, \quad (0,1) + K, \quad (0,2) + K,$$
$$(1,0) + K, \quad (1,1) + K, \quad (1,2) + K.$$

Furthermore, these six cosets are distinct.

Two cosets $a + K$ and $b + K$ are equal only if $a - b \in K$, which cannot happen for any pair of cosets in this list.

Addition of these cosets corresponds to adding the first components of the representatives modulo 2 and the second components modulo 3. To be precise, the function ϕ defined by

$$\phi : (\mathbb{Z} \times \mathbb{Z})/K \to \mathbb{Z}_2 \times \mathbb{Z}_3$$
$$(m, n) + K \mapsto (m, n)$$

is an isomorphism.

Thus A is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$. ♦

We now describe the process that we have used in Example 1.1 in a way that we can generalize.

We were given a presentation with a finite number of generators

In our specific example this was two.

$$a_1, \ldots, a_n$$

and a finite number of relations

Also two.

$$w_1 = 0, \ldots, w_m = 0,$$

where each w_i was of the form

$$w_i = p_{i1}a_1 + \cdots + p_{in}a_n.$$

Using this generalized notation, the group A in Example 1.1 becomes

$$A = \langle a_1, a_2 : \ w_1 = 0, \ w_2 = 0 \rangle,$$

where

$$w_1 = 2a_1 + 0a_2,$$
$$w_2 = 0a_1 + 3a_2;$$

that is,

$$p_{11} = 2, \quad p_{12} = 0,$$
$$p_{21} = 0, \quad p_{22} = 3.$$

The elements of $\mathbb{Z} \times \mathbb{Z}$ corresponding to the words w_1 and w_2 are (p_{11}, p_{12}) and (p_{21}, p_{22}).

Following the above example, we can now give a formal definition of what we mean when we define an Abelian group A by a *finite presentation* with n generators,

$$a_1, \ldots, a_n,$$

and m relations,

$$w_1 = 0, \quad \ldots, \quad w_m = 0,$$

where each relation is of the form

$$w_i = p_{i1}a_1 + \cdots + p_{in}a_n = 0, \quad p_{ij} \in \mathbb{Z}, \quad j = 1, \ldots, n.$$

In our usual notation

$$A = \langle a_1, \ldots, a_n : \ w_1 = 0, \ \ldots, \ w_m = 0 \rangle.$$

Following the example, we take the free Abelian group on n generators in its concrete form as a direct product of n copies of $\mathbb{Z}$.

That is, with the same number of generators as A.

We then form the smallest subgroup K of this direct product containing the elements corresponding to the relations. That is, K is the smallest subgroup containing the elements

$$(p_{11}, \ldots, p_{1n}),$$
$$\vdots$$
$$(p_{m1}, \ldots, p_{mn}).$$

Finally, A is *defined* to be the quotient group of the direct product $\mathbb{Z} \times \cdots \times \mathbb{Z}$ (of n copies of $\mathbb{Z}$) by the subgroup K.

Expressing this process symbolically for the general case we have the following.

Definition 1.2 Finitely presented Abelian group

The **finitely presented Abelian group** A with **(finite) presentation**

$$\langle a_1, \ldots, a_n : \ w_1 = 0, \ \ldots, \ w_m = 0 \rangle,$$

where

$$w_i = p_{i1}a_1 + \cdots + p_{in}a_n, \quad p_{ij} \in \mathbb{Z}, \quad i = 1, \ldots, m, \ j = 1, \ldots, n,$$

is defined to be

$$A = (\overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n \text{ copies}})/K,$$

where K is the smallest subgroup of

$$\overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n \text{ copies}}$$

containing the elements

$$(p_{11}, \ldots, p_{1n}), \ldots, (p_{m1}, \ldots, p_{mn}).$$

Such presentations are called 'finite' because they involve only finitely many generators and finitely many relations.

This definition corresponds to the more general one given in *Unit IB4* with the following changes:

(a) the free group on n generators becomes the free *Abelian* group on n generators;

(b) the normality of the subgroup generated by the words corresponding to the relations is automatic.

In the notation we have used, the Abelian group

$$A = \langle a_1, \ldots, a_n : w_1 = 0, \ \ldots, \ w_m = 0\rangle$$

is completely determined by the $m \times n$ integers

$$p_{ij}, \quad i = 1, \ldots, m, \ j = 1, \ldots, n.$$

These integers, in turn, define an $m \times n$ matrix

$$\mathbf{P} = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix},$$

with integer entries. We shall refer to such matrices as **integer matrices**.

Notational convention

We often shorten the above notation for the matrix $\mathbf{P}$ to

$$\mathbf{P} = [p_{ij}].$$

We shall usually adhere to the convention that the elements of a matrix will be denoted by the italic lower-case letter corresponding to the bold upper-case letter used for the matrix itself.

The integer matrix corresponding to the presentation of Example 1.1, namely

$$A = \langle a, b : \ 2a = 0, \ 3b = 0\rangle,$$

is

$$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}.$$

The elements 2 and 3 in this diagonal matrix lead to the result that the group A is, in this case, $\mathbb{Z}_2 \times \mathbb{Z}_3$.

We shall often write 'is' where we should perhaps write 'is isomorphic to'.

Exercise 1.4

Write down the integer matrices corresponding to the following finite presentations of Abelian groups:

(a) $A = \langle a_1, a_2, a_3 : \ 3a_1 + 2a_2 = 0, \ 2a_2 - 5a_3 = 0, \ 6a_1 - 3a_3 = 0\rangle$;

(b) $A = \langle a_1, a_2, a_3 : \ 4a_1 - 2a_2 = 0, \ 6a_1 - 3a_3 = 0\rangle$;

(c) $A = \langle a_1, a_2 : \ 3a_1 + 2a_2 = 0, \ 2a_1 - 5a_2 = 0, \ 6a_1 - 3a_2 = 0\rangle$.

In general, for square matrices, if the integer matrix corresponding to the relations is diagonal, with positive diagonal entries, we can immediately describe the group as a direct product of cyclic groups in a way that is made precise in the following theorem.

Theorem 1.2

If A is a finitely presented Abelian group with presentation

$$A = \langle a_1, \ldots, a_n : \; d_1 a_1 = 0, \; \ldots, \; d_n a_n = 0 \rangle,$$

where

$$d_i \in \mathbb{Z}, \quad d_i > 0, \quad i = 1, \ldots, n,$$

then

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}.$$

We are *not* going to present a formal proof of this theorem because the technical details that are required in the proof do not shed any further light on the result.

However, from an intuitive point of view, the result is entirely reasonable. Defining A as a quotient with respect to K means that we calculate in A in the same way as in

$$\overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n \text{ copies}}$$

except that we treat elements of K as zero.
Since K contains the element

$$(d_1, 0, \ldots, 0),$$

this means that addition in the first coordinate is done modulo d_1. Similarly, addition in the ith coordinate is done modulo d_i. Hence

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n},$$

as claimed.

We can extend this result on diagonal matrices to allow for zeros on the diagonal. If such a zero appears, it corresponds to a relation $0a_i = 0$, which is always satisfied. Such a relation imposes no restrictions and so there is no reduction in the corresponding $\mathbb{Z}$. For example, the integer matrix

$$\begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$$

gives rise to the direct product

$$\mathbb{Z}_2 \times \mathbb{Z}.$$

Exercise 1.5

For each of the following finite presentations of Abelian groups, write down the corresponding integer matrix and express the group defined as a direct product of cyclic groups:

(a) $A = \langle a, b : \; 2a = 0, \; 7b = 0 \rangle$;

(b) $A = \langle a, b, c : \; 4a = 0, \; 6b = 0, \; 5c = 0 \rangle$.

For examples with small numbers of generators it is easier to write

$$a, b, c, \ldots$$

rather than

$$a_1, a_2, a_3, \ldots,$$

and we shall usually do so.

The main objective of this unit is to identify a finitely presented Abelian group from the matrix of its presentation. So far we can only do this for a presentation giving rise to a diagonal square matrix with non-negative entries.

Not all of the matrices derived from presentations are square, as you saw in Exercise 1.4. We extend our result by firstly considering *non-square* diagonal matrices with non-negative entries, that is matrices

The following are examples of non-square diagonal matrices:

$$\begin{bmatrix} 2 & 0 \\ 0 & 5 \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \end{bmatrix}.$$

$$\mathbf{P} = [p_{ij}]$$

with

$$p_{ii} \geq 0, \quad p_{ij} = 0, \, i \neq j.$$

Remember that, from the way we defined the matrix corresponding to a presentation, the number of columns in the matrix is the number of generators, while the number of rows is the number of relations.

Firstly, consider a diagonal matrix such as

$$\begin{bmatrix} 2 & 0 \\ 0 & 5 \\ 0 & 0 \end{bmatrix},$$

with more rows than columns. This represents an Abelian group with two generators, three relations and presentation

$$A = \langle a, b \colon \, 2a + 0b = 0, \; 0a + 5b = 0, \; 0a + 0b = 0 \rangle.$$

Since the third relation is automatically satisfied it tells us nothing about A. The group A is exactly the same as the Abelian group with presentation

$$\langle a, b \colon \, 2a = 0, \; 5b = 0 \rangle.$$

Hence,

$$A \cong \mathbb{Z}_2 \times \mathbb{Z}_5.$$

In general, if a diagonal matrix has 'extra' rows then these extra rows can only contain zeros. The corresponding relations give no information and the rows may simply be ignored.

Secondly, consider the diagonal matrix

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \end{bmatrix},$$

with more columns than rows. This represents an Abelian group with three generators, two relations and presentation

$$A = \langle a, b, c \colon \, 2a + 0b + 0c = 0, \; 0a + 5b + 0c = 0 \rangle.$$

The group A is exactly the same as the Abelian group given by the presentation

$$\langle a, b, c \colon \, 2a = 0, \; 5b = 0 \rangle.$$

Since there are three generators, our group A is a quotient of the free Abelian group

There are three columns in the matrix.

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}.$$

We argue, as in the square case, that, because of the relation $2a = 0$, the first component of the quotient reduces to $\mathbb{Z}_2$.
Similarly, because of the relation $5b = 0$, the second component of the quotient reduces to $\mathbb{Z}_5$.
Because there is *no* relation involving the third generator, there is no reduction of the third component, which remains as $\mathbb{Z}$.
Hence,

$$A \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}.$$

The number of columns in the matrix tells us how many copies of $\mathbb{Z}$ we start with. The number of 'extra' columns tells us how many $\mathbb{Z}$s are *not* reduced.

Generalizing these examples, we can now interpret any diagonal matrix with non-negative entries corresponding to a finite presentation of an Abelian group. We can express the group as a direct product of cyclic groups. Each component in the direct product is either $\mathbb{Z}_k$, for some positive integer k, or $\mathbb{Z}$.

We now extend the result for diagonal matrices to include negative elements on the diagonal.

If $ka = 0$ then $-ka = 0$ and conversely. Hence a relation of the form

$$ka = 0, \quad k < 0, k \in \mathbb{Z},$$

has exactly the same effect as the relation

$$-ka = 0, \quad (-k) > 0,$$

and hence gives rise to a component

$$\mathbb{Z}_{-k} = \mathbb{Z}_{|k|}.$$

Exercise 1.6

Each of the following matrices represents a finite presentation of an Abelian group. In each case, write down the corresponding presentation and express the group as a direct product of cyclic groups.

(a) $\begin{bmatrix} 5 & 0 & 0 \\ 0 & 7 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

(b) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}$

(c) $\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & -5 & 0 & 0 \\ 0 & 0 & 7 & 0 \end{bmatrix}$

(d) $\begin{bmatrix} -3 & 0 & 0 \\ 0 & 11 & 0 \\ 0 & 0 & -13 \\ 0 & 0 & 0 \end{bmatrix}$

We now know how to to deal with any diagonal matrix corresponding to a finite presentation of an Abelian group:

(a) any negative element on the diagonal is replaced by its modulus;

(b) any 'extra' row, which must contain only zeros, is ignored;

(c) each positive entry k on the diagonal gives rise to a component $\mathbb{Z}_k$;

(d) each zero entry on the diagonal gives rise to a component $\mathbb{Z}$;

(e) any 'extra' column gives rise to a component $\mathbb{Z}$.

You might have wondered why we are considering matrices with rows of zeros, or zeros on the diagonal. A presentation would not normally contain the corresponding trivial relation. Our reason for doing so is that we shall show that a finite presentation with a corresponding *non-diagonal* matrix can also be described by a diagonal matrix. This corresponding diagonal matrix may have 'extra' rows, or zeros on the diagonal, which we need to be able to interpret.

In the next section we shall give a method of reducing a non-diagonal matrix to diagonal form in a way which does not change the Abelian group represented.

2 THE REDUCTION ALGORITHM

In this section we shall describe an algorithm for reducing the matrix representing a finitely presented Abelian group to diagonal form. We leave the justification of why this algorithm must lead to a diagonal matrix and why the group represented remains unchanged until Section 3 of this unit. The purpose of this section is to get you used to using the algorithm and interpreting the results. The operations that we are going to perform on matrices are 'elementary row and column operations', which you may have met in previous courses.

The *elementary row operations* we shall use are the following:

1 change the sign of a row (that is, multiply it by -1);

2 interchange two rows;

3 add an *integer* multiple of one row to another row.

We shall use the following notation to describe these operations:

$$\begin{aligned} R_i &\to -R_i && \text{change sign of } i\text{th row;} \\ R_i &\leftrightarrow R_j && \text{interchange } i\text{th and } j\text{th rows;} \\ R_i &\to R_i + kR_j && \text{add } k \text{ times } j\text{th row to } i\text{th}, j \neq i. \end{aligned}$$

You may wish to read → as 'is replaced by' or 'becomes'.

The corresponding *elementary column operations* we shall use are:

1 change the sign of a column (that is, multiply it by -1);

2 interchange two columns;

3 add an *integer* multiple of one column to another column.

We shall use the notation corresponding to that above, with Rs replaced by Cs, for elementary column operations.

It will be clear from the context when we are using C_i for a column and when for a cyclic group with i elements.

If you have met elementary operations on matrices before, note that here we restrict them in two ways:

(a) in the first type of operation only the multiplier -1 is allowed;

(b) in the third type of operation only *integer* multiples are allowed.

We shall take up the reasons for these restrictions later.

The following example illustrates how to diagonalize a matrix using these elementary operations.

Example 2.1

Consider the finitely presented Abelian group A defined by

$$A = \langle a_1, a_2 : \; 8a_1 + 6a_2 = 0, \; 5a_1 + 3a_2 = 0 \rangle.$$

The corresponding matrix is

$$\begin{bmatrix} 8 & 6 \\ 5 & 3 \end{bmatrix}.$$

It is not difficult to reduce this to a diagonal matrix using the elementary operations. One such reduction is as follows.

$$\begin{aligned} \begin{bmatrix} 8 & 6 \\ 5 & 3 \end{bmatrix} &\mapsto \begin{bmatrix} -2 & 0 \\ 5 & 3 \end{bmatrix} && R_1 \to R_1 + (-2)R_2 \\ &\mapsto \begin{bmatrix} 2 & 0 \\ 5 & 3 \end{bmatrix} && R_1 \to -R_1 \\ &\mapsto \begin{bmatrix} 2 & 0 \\ 3 & 3 \end{bmatrix} && R_2 \to R_2 + (-1)R_1 \\ &\mapsto \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} && C_1 \to C_1 + (-1)C_2 \end{aligned}$$

♦

Exercise 2.1

Assuming that elementary operations on the matrix of a presentation do not change the group, identify the Abelian group A defined by

$$A = \langle a_1, a_2 : \; 8a_1 + 6a_2 = 0, \; 5a_1 + 3a_2 = 0 \rangle$$

as a direct product of cyclic groups.

Had we asked *you* to reduce the matrix in Example 2.1 to a diagonal matrix using elementary row and column operations, you might well have come up with an entirely different sequence of operations. This thought should lead you to ask two questions.

(a) Is it possible to arrive at different diagonal matrices by using different choices for the elementary operations?

(b) Is there any systematic method of choosing the elementary operations which will guarantee reduction to diagonal form?

The answer to the first question is 'yes'. For example, it is also possible to reduce the matrix

$$\begin{bmatrix} 8 & 6 \\ 5 & 3 \end{bmatrix}$$

to the diagonal matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}.$$

The next exercise provides a justification of why this is possible (without telling you how to do it).

Exercise 2.2

What Abelian group is represented by the diagonal matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}?$$

Explain why this is the same group as that represented by the matrix

$$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}.$$

We shall from now on often say that two groups are 'the same' if they are 'the same up to isomorphism'.

The answer to the second question is also 'yes'. The algorithm which we are about to discuss justifies this. We shall refer to this algorithm as the *Reduction Algorithm*.

The algorithm consists of an inner loop and an outer loop. The inner loop creates *one* diagonal element. The outer loop causes the inner loop to be repeated so that *all* the diagonal elements are created, one at a time.

The inner loop consists of two steps.

1 Interchange rows and/or columns to place the element with the smallest non-zero magnitude in the top left-hand corner. Change the sign of the first row, if necessary, to ensure that the element in the top left-hand corner is positive. Denote this element by q.

2 (a) If q divides every other element in the first row and column, add integer multiples of the first row/column to the other rows/columns to reduce the off-diagonal elements in the first row and column to zeros.

(b) If q does not divide every other element in the first row and column, choose any element in the first row or column not divisible by q and add an integer multiple of the first row/column to the row/column containing the chosen element to reduce it to its remainder modulo q. Interchange two rows or columns to place the remainder in the top left-hand corner. Label this remainder q and repeat step 2.

Once the inner loop has been completed, ending with an application of step 2(a), one diagonal element has been created (i.e. the only non-zero element in the first row and column is in the top left-hand corner).

The outer loop consists of applying the inner loop several times until the only non-zero elements lie along the diagonal of the matrix. Firstly, it tells us to apply the inner loop to the whole matrix, to give us a matrix of the form

$$\begin{bmatrix} q_1 & 0 \dots 0 \\ 0 & \\ \vdots & \text{submatrix} \\ 0 & \end{bmatrix}.$$

Next, it tells us to apply the inner loop again to the submatrix, to give us a matrix of the form

$$\begin{bmatrix} q_1 & 0 & 0 \dots 0 \\ 0 & q_2 & 0 \dots 0 \\ 0 & 0 & \\ \vdots & \vdots & \text{submatrix} \\ 0 & 0 & \end{bmatrix}.$$

The application of elementary operations to the rows and columns of submatrices has the same effect as applying these operations to the whole matrix because of the zeros that have been created at previous applications of the inner loop.

We continue in this way, applying the inner loop to each submatrix in turn, until we get a diagonal matrix, at which point we stop.

The following examples illustrate how the algorithm works.

Example 2.2

We illustrate the process firstly for the matrix from Example 2.1:

$$\begin{bmatrix} 8 & 6 \\ 5 & 3 \end{bmatrix}.$$

The reduction proceeds as follows.

Obtain first diagonal element

The element of smallest non-zero magnitude is 3, so we start by bringing this to the top left-hand corner.

$$\begin{aligned}
\begin{bmatrix} 8 & 6 \\ 5 & 3 \end{bmatrix} &\mapsto \begin{bmatrix} 5 & 3 \\ 8 & 6 \end{bmatrix} && R_1 \leftrightarrow R_2 \\
&\mapsto \begin{bmatrix} 3 & 5 \\ 6 & 8 \end{bmatrix} && C_1 \leftrightarrow C_2 \\
&\mapsto \begin{bmatrix} 3 & 2 \\ 6 & 2 \end{bmatrix} && C_2 \to C_2 + (-1)C_1 \quad \text{(reduce 5 mod 3)} \\
&\mapsto \begin{bmatrix} 2 & 3 \\ 2 & 6 \end{bmatrix} && C_1 \leftrightarrow C_2 \quad \text{(smallest to top left)} \\
&\mapsto \begin{bmatrix} 2 & 1 \\ 2 & 4 \end{bmatrix} && C_2 \to C_2 + (-1)C_1 \quad \text{(reduce 3 mod 2)} \\
&\mapsto \begin{bmatrix} 1 & 2 \\ 4 & 2 \end{bmatrix} && C_1 \leftrightarrow C_2 \quad \text{(smallest to top left)} \\
&\mapsto \begin{bmatrix} 1 & 0 \\ 4 & -6 \end{bmatrix} && C_2 \to C_2 + (-2)C_1 \quad \text{(reduce 2 mod 1)} \\
&\mapsto \begin{bmatrix} 1 & 0 \\ 0 & -6 \end{bmatrix} && R_2 \to R_2 + (-4)R_1 \quad \text{(reduce 4 mod 1)}
\end{aligned}$$

1 divides all elements in first row and column

Obtain second diagonal element

The submatrix here is just $[-6]$, and so all we have to do is to make this element positive.

$$\begin{bmatrix} 1 & 0 \\ 0 & -6 \end{bmatrix} \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix} \qquad R_2 \leftrightarrow -R_2 \qquad ♦$$

Example 2.3

The matrix we shall consider this time is

$$\begin{bmatrix} 0 & 10 & 15 \\ 6 & 10 & 0 \\ 6 & 0 & 15 \end{bmatrix}.$$

Obtain first diagonal element

The smallest non-zero magnitude among the elements is 6.

$$\begin{bmatrix} 0 & 10 & 15 \\ 6 & 10 & 0 \\ 6 & 0 & 15 \end{bmatrix} \mapsto \begin{bmatrix} 6 & 10 & 0 \\ 0 & 10 & 15 \\ 6 & 0 & 15 \end{bmatrix} \qquad R_1 \leftrightarrow R_2$$

$$\mapsto \begin{bmatrix} 6 & 4 & 0 \\ 0 & 10 & 15 \\ 6 & -6 & 15 \end{bmatrix} \qquad C_2 \to C_2 - C_1 \quad \text{(reduce 10 mod 6)}$$

$$\mapsto \begin{bmatrix} 4 & 6 & 0 \\ 10 & 0 & 15 \\ -6 & 6 & 15 \end{bmatrix} \qquad C_1 \leftrightarrow C_2$$

$$\mapsto \begin{bmatrix} 4 & 2 & 0 \\ 10 & -10 & 15 \\ -6 & 12 & 15 \end{bmatrix} \qquad C_2 \to C_2 - C_1$$

$$\mapsto \begin{bmatrix} 2 & 4 & 0 \\ -10 & 10 & 15 \\ 12 & -6 & 15 \end{bmatrix} \qquad C_1 \leftrightarrow C_2$$

$$\mapsto \begin{bmatrix} 2 & 0 & 0 \\ -10 & 30 & 15 \\ 12 & -30 & 15 \end{bmatrix} \qquad C_2 \to C_2 - 2C_1$$

$$\mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & 30 & 15 \\ 12 & -30 & 15 \end{bmatrix} \qquad R_2 \to R_2 + 5R_1$$

$$\mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & 30 & 15 \\ 0 & -30 & 15 \end{bmatrix} \qquad R_3 \to R_3 - 6R_1$$

Obtain second diagonal element

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 30 & 15 \\ 0 & -30 & 15 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & 15 & 30 \\ 0 & 15 & -30 \end{bmatrix} \qquad C_2 \leftrightarrow C_3$$

$$\mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & 15 & 0 \\ 0 & 15 & -60 \end{bmatrix} \qquad C_3 \to C_3 - 2C_2$$

$$\mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & 15 & 0 \\ 0 & 0 & -60 \end{bmatrix} \qquad R_3 \to R_3 - R_2$$

15 divides all elements in first row and column of submatrix $\begin{bmatrix} 15 & 30 \\ 15 & -30 \end{bmatrix}$.

Obtain third diagonal element

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 15 & 0 \\ 0 & 0 & -60 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & 15 & 0 \\ 0 & 0 & 60 \end{bmatrix} \qquad R_3 \to -R_3 \qquad \blacklozenge$$

Exercise 2.3

Assuming that elementary operations on the matrix of a presentation do not change the group, use Example 2.3 to help you identify the Abelian group A defined by

$$A = \langle a_1, a_2, a_3 : \ 10a_2 + 15a_3 = 0, \ 6a_1 + 10a_2 = 0, \ 6a_1 + 15a_3 = 0 \rangle$$

as a direct product of cyclic groups.

In Examples 2.2 and 2.3, at several steps we had a choice in terms of which elementary operation we could apply. For example, in Example 2.2, when we obtained the matrix

$$\begin{bmatrix} 3 & 5 \\ 6 & 8 \end{bmatrix}$$

we had a choice of applying

$$C_2 \to C_2 + (-1)C_1 \quad \text{or} \quad R_2 \to R_2 + (-2)R_1,$$

and we chose the former. It turns out, as we shall see in Section 3, that the choices we make do not matter, since the diagonal matrix we end up with will always represent the same group (up to isomorphism) as the following exercise illustrates.

Exercise 2.4

(a) Complete the reduction in Example 2.3 from the point at which the matrix has been reduced to

$$\begin{bmatrix} 4 & 6 & 0 \\ 10 & 0 & 15 \\ -6 & 6 & 15 \end{bmatrix}$$

by reducing the 10 in the first column instead of the 6 in the first row, and then making any further choices as you wish.

(b) Identify the group represented by the resulting diagonal matrix.

(c) Justify why the two groups obtained from the different diagonal forms are the same (up to isomorphism).

The results of Exercises 2.1–2.4 show that the application of the Reduction Algorithm does not necessarily lead to a unique expression for a group as a direct product of cyclic groups. In the cases where we have arrived at two different matrices, however, our knowledge of cyclic groups has shown us why the resulting direct products are isomorphic. We shall later show how to use this knowledge of cyclic groups to express each product in a standard or *canonical* form, which *is* unique.

Exercise 2.5

Assuming that elementary operations on the matrix of a presentation do not change the group, identify the Abelian group A defined by

$$A = \langle a_1, a_2, a_3 : \ 3a_1 + 2a_2 + 4a_3 = 0, \ 6a_1 + a_2 + 7a_3 = 0, \\ 2a_1 + 3a_2 + 6a_3 = 0 \rangle$$

as a direct product of cyclic groups.

3 PROOF OF THE REDUCTION ALGORITHM (AUDIO-TAPE SECTION)

In Section 2 you saw how to apply the Reduction Algorithm to diagonalize an integer matrix derived from a finite presentation of an Abelian group. The resulting diagonal matrix enabled you to express the group as a direct product of cyclic groups.

A complete description of the Reduction Algorithm is as follows.

Reduction algorithm

Given any $m \times n$ integer matrix, apply the following two steps first to the whole matrix, then to the submatrix obtained by ignoring the first row and column of the matrix, then to the submatrix obtained by ignoring the first row and column of the previous submatrix, and so on, until a diagonal matrix is obtained.

1 Interchange rows and/or columns to place the element with the smallest non-zero magnitude in the top left-hand corner. Change the sign of the first row, if necessary, to ensure that the element in the top left-hand corner is positive. Denote this element by q.

2 (a) If q divides every other element in the first row and column, add integer multiples of the first row/column to the other rows/columns to reduce the off-diagonal elements in the first row and column to zeros.

(b) If q does not divide every other element in the first row and column, choose any element in the first row or column not divisible by q and add an integer multiple of the first row/column to the row/column containing the chosen element to reduce it to its remainder modulo q. Interchange two rows or columns to place the remainder in the top left-hand corner. Label this remainder q and repeat step 2.

If all the matrix entries are zero, then the matrix is already in diagonal form and so the algorithm stops before it starts.

This section contains two major results. In the audio programme and tape frames, we shall justify why the Reduction Algorithm works. This involves showing two things: firstly, that the process will eventually terminate and produce a diagonal matrix; secondly, that the resulting diagonal matrix represents the same Abelian group as the original presentation. Then, after the audio work, we shall state a theorem which asserts that a finitely presented Abelian group can be written uniquely as a direct product in canonical form (though we shall postpone the proof of this theorem until Section 4).

We use the same notation as in Section 1. The Abelian group A is given by the finite presentation

$$A = \langle a_1, \ldots, a_n : w_1 = 0, \ldots, w_m = 0 \rangle,$$

where

$$\begin{aligned} w_1 &= p_{11}a_1 + \cdots + p_{1n}a_n \\ &\vdots \\ w_m &= p_{m1}a_1 + \cdots + p_{mn}a_n \end{aligned}$$

The matrix to be diagonalized is

$$\mathbf{P} = [p_{ij}] = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix}.$$

There is one very easy case of such a presentation: the one where the matrix **P** consists entirely of zeros. In this case there are no relations and we simply have the free Abelian group corresponding to the number of generators. What is more, the matrix is already reduced to diagonal form. Throughout the audio programme, therefore, we shall assume that we begin with a matrix **P** having at least one non-zero entry.

You should now listen to the audio programme for this unit, referring to the tape frames below when asked to during the programme.

1

Overview

Aim

(a) Algorithm results in a diagonal matrix ...

(b) ... which represents the same group

Strategy

(a) Each elementary operation provides a 'simpler' matrix

(b) Each elementary operation preserves the group

2

The group

$A = \langle a_1, \ldots, a_n : w_1 = 0, \ldots, w_m = 0 \rangle$

$A = F/H$

F free Abelian group with generators $a_1, \ldots, a_n$

H subgroup with generators $w_1, \ldots, w_m$

$$\begin{array}{l} w_1 = p_{11}a_1 + \cdots + p_{1n}a_n \\ \vdots \\ w_m = p_{m1}a_1 + \cdots + p_{mn}a_n \end{array}$$

3

A in terms of the $m \times n$ matrix $\mathbf{P}$

$$A = (\underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n \text{ copies}})/H$$

H is the subgroup generated by the m rows of $\mathbf{P}$, i.e.

$$\begin{array}{c} (p_{11}, \ldots, p_{1n}) \\ (p_{21}, \ldots, p_{2n}) \\ \vdots \\ (p_{m1}, \ldots, p_{mn}) \end{array}$$

4

Row operations

$R_1 \to -R_1$

change generators of H

Old word: $w_1 = p_{11}a_1 + \cdots + p_{1n}a_n$

New word: $w_1' = -p_{11}a_1 - \cdots - p_{1n}a_n$

$= -w_1$

5

Groups, new and old

Old: $A = F/H$ $H = \langle w_1, \ldots, w_m \rangle$

New: $A' = F/H'$ $H' = \langle w_1', \ldots, w_m' \rangle$
where $w_1' = -w_1$, $w_i' = w_i$, $i = 2, \ldots, m$

To get $A' = A$, will show $H' = H$

6

The particular case

$w_1' = -w_1$

As $w_1 \in \langle w_1, \ldots, w_m \rangle = H$,

$w_1' = -w_1 \in H$ (H is a subgroup)

So $\{w_1', \ldots, w_m'\} \subseteq H$, $\quad$ giving $H' = \langle w_1', \ldots, w_m' \rangle \subseteq H$

$w_1 = -w_1'$

As $w_1' \in \langle w_1', \ldots, w_m' \rangle = H'$,

$w_1 = -w_1' \in H'$ (H′ is a subgroup)

So $\{w_1, \ldots, w_m\} \subseteq H'$ $\quad$ giving $H = \langle w_1, \ldots, w_m \rangle \subseteq H'$

Hence $H' = H$ and $A' = A$

7

General strategy

For any elementary row operation with

old words: $\quad w_1, \ldots, w_m$

new words: $\quad w_1', \ldots, w_m'$

Show $\{w_1', \ldots, w_m'\} \subseteq H$ $\quad$ giving $H' = \langle w_1', \ldots, w_m' \rangle \subseteq H$

and $\{w_1, \ldots, w_m\} \subseteq H'$ $\quad$ giving $H = \langle w_1, \ldots, w_m \rangle \subseteq H'$

So $H' = H$ and $A' = F/H' = F/H = A$

8

Exercise 3.1

Describe, in terms of the old words, the new words generated by each of the three types of elementary row operation:

(a) $R_i \longrightarrow -R_i$

(b) $R_i \longleftrightarrow R_j$

(c) $R_i \longrightarrow R_i + kR_j$

8A

Solution 3.1

Old words: $\quad w_1, \ldots, w_m$

(a) $R_i \longrightarrow -R_i$

New words: $\quad w_i' = -w_i, \quad w_h' = w_h, \quad h \neq i$

(b) $R_i \longleftrightarrow R_j$

New words: $\quad w_i' = w_j, \; w_j' = w_i, \quad w_h' = w_h, \quad h \neq i, j$

(c) $R_i \longrightarrow R_i + kR_j$

New words: $\quad w_i' = w_i + kw_j, \quad w_h' = w_h, \quad h \neq i$

9

Exercise 3.2

Verify, for each of the three types of elementary row operation, that $H' = H$ and so $A' = A$

9A

Solution 3.2

(a) Since $w_i \in H$,
$w_i' = -w_i \in H$

So $\{w_1', \ldots, w_m'\} \subseteq H$
and $H' \subseteq H$

Since $w_i' \in H'$,
$w_i = -w_i' \in H'$

the operation is reversible

So $\{w_1, \ldots, w_m\} \subseteq H'$
and $H \subseteq H'$

Hence $H' = H$ and $A' = A$

(b) The only change is that the *w*s appear in a different order

So $\{w_1', \ldots, w_m'\} = \{w_1, \ldots, w_m\}$
and the result is immediate

(c) Since $w_i \in H$ and $w_j \in H$,
$w_i' = w_i + kw_j \in H$

So $\{w_1', \ldots, w_m'\} \subseteq H$
and $H' \subseteq H$

Since $w_i' = w_i + kw_j \in H'$ and $w_j' = w_j \in H'$,
$w_i' - kw_j' = w_i \in H'$

the operation is reversible

So $\{w_1, \ldots, w_m\} \subseteq H'$
and $H \subseteq H'$

Hence $H' = H$ and $A' = A$

This concludes the proof that the group defined is unchanged by any of the three types of elementary row operation

10

Column operations

$C_i \to -C_i$

New words:

$$
\begin{aligned}
w_1' &= p_{11}a_1 + \cdots + p_{1i-1}a_{i-1} - p_{1i}a_i + p_{1i+1}a_{i+1} + \cdots + p_{1n}a_n \\
&\;\;\vdots \\
w_m' &= p_{m1}a_1 + \cdots + p_{mi-1}a_{i-1} - p_{mi}a_i + p_{mi+1}a_{i+1} + \cdots + p_{mn}a_n
\end{aligned}
$$

Rearranged as:

$$
\begin{aligned}
w_1' &= p_{11}a_1 + \cdots + p_{1i-1}a_{i-1} + p_{1i}(-a_i) + p_{1i+1}a_{i+1} + \cdots + p_{1n}a_n \\
&\;\;\vdots \\
w_m' &= p_{m1}a_1 + \cdots + p_{mi-1}a_{i-1} + p_{mi}(-a_i) + p_{mi+1}a_{i+1} + \cdots + p_{mn}a_n
\end{aligned}
$$

Same words but on new generators

$a_i' = -a_i\,, \quad a_h' = a_h,\ h \neq i$

We need to show $a_1', \ldots, a_n'$ generate same F

11

The n new a's generate the same F

$a_i' = -a_i \in F$ because F is a group

So $F' = \langle a_1', \ldots, a_n' \rangle \subseteq F$

Conversely, $a_i = -a_i' \subseteq F'$

So $F = \langle a_1, \ldots, a_n \rangle \subseteq F'$

Hence $F = F'$

and both $\{a_1, \ldots, a_n\}$ and $\{a_1', \ldots, a_n'\}$ generate F

So, from Frame 10, $H' = H$ and $A' = A$

12

Exercise 3.3

Describe, in terms of the old generators, the new generators $a_1', \ldots, a_n'$ corresponding to the second and third types of elementary column operation:

(b) $C_i \leftrightarrow C_j$

(c) $C_i \to C_i + kC_j$

choose the generators to preserve the words

12A

Solution 3.3

(b) $a_i' = a_j, \quad a_j' = a_i, \quad a_h' = a_h,\ h \neq i, j$

(c) $a_j' = a_j + ka_i, \quad a_h' = a_h,\ h \neq j$

Surprise! It's a_j that has to change, not a_i!

To see why, consider any word, e.g. the first
$w_1 = p_{11}a_1 + \cdots + p_{1i}a_i + \cdots + p_{1j}a_j + \cdots + p_{1n}a_n$

This becomes
$p_{11}a_1 + \cdots + (p_{1i} + kp_{1j})a_i + \cdots + p_{1j}a_j + \cdots + p_{1n}a_n$

which can be rearranged as
$p_{11}a_1 + \cdots + p_{1i}a_i + \cdots + p_{1j}(a_j + ka_i) + \cdots + p_{1n}a_n$

This looks just like the original word,
apart from the new generator in the jth place

13

Completing the proof

The new generators corresponding to the second and third types of elementary column operation generate the same F, by an argument like that in Frame 9A(b) and (c)

Also, our choice of new generators ensures that the forms of the words are unchanged

Hence the quotient group A is unchanged

14

The algorithm terminates in a diagonal matrix

Reduce **P** to the form

$$\left[\begin{array}{c|c} \times & 0 \quad \cdot \quad \cdot \quad \cdot \quad 0 \\ \hline 0 & \\ \vdots & (m-1) \times (n-1) \\ \vdots & \text{submatrix} \\ 0 & \end{array}\right]$$

Now repeat for the $(m-1) \times (n-1)$ submatrix
And so on ...

If **P** is square, process terminates with a diagonal matrix
If not, final procedure as below

15

The case $m < n$

The process would reach a stage like this:

$$\begin{bmatrix} q_1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & q_2 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & q_{m-1} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \multicolumn{3}{c}{\underbrace{\boxed{p'_{mm} \qquad p'_{mn}}}} \end{bmatrix}$$

if all zeros, finished

if not, reduce $(p'_{mm} \ \cdots \ p'_{mn})$

16

Final step of algorithm if $m < n$

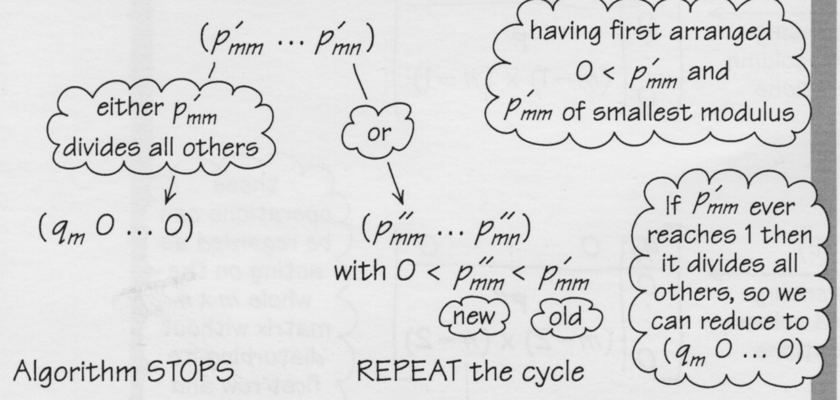
Reduce row matrix $(p'_{mm} \cdots p'_{mn})$

to $(q_m \ 0 \ \ldots \ 0)$

by elementary column operations

17

Cycle for a row matrix



$(p'_{mm} \cdots p'_{mn})$

either p'_{mm} divides all others

or

having first arranged $0 < p'_{mm}$ and p'_{mm} of smallest modulus

$(q_m \ 0 \ldots 0)$

$(p''_{mm} \cdots p''_{mn})$

with $0 < \underset{\text{new}}{p''_{mm}} < \underset{\text{old}}{p'_{mm}}$

If p'_{mm} ever reaches 1 then it divides all others, so we can reduce to $(q_m \ 0 \ldots 0)$

Algorithm STOPS

REPEAT the cycle

Process must terminate in at most p'_{mm} iterations

18

The case $m > n$

$$\begin{bmatrix} q_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & q_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \ddots & & \vdots & \vdots \\ \vdots & \vdots & & & 0 & 0 \\ 0 & 0 & \cdots & 0 & q_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & 0 & p'_{nn} \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & p'_{mn} \end{bmatrix}$$

column matrix $\begin{bmatrix} p'_{nn} \\ \vdots \\ p'_{mn} \end{bmatrix}$

19

Basic step of algorithm for $m \times n$ matrix

$$\begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{m1} & \cdots & p_{mn} \end{bmatrix}$$

having first arranged $0 < p_{11}$ and p_{11} of smallest modulus

either

$$\begin{bmatrix} q_1 & 0 & \cdots & 0 \\ 0 & p'_{22} & \cdots & p'_{2n} \\ \vdots & \vdots & & \vdots \\ 0 & p'_{m2} & \cdots & p'_{mn} \end{bmatrix}$$

Step COMPLETE

or

$$\begin{bmatrix} p'_{11} & \cdots & p'_{1n} \\ \vdots & & \vdots \\ p'_{m1} & \cdots & p'_{mn} \end{bmatrix}$$

with $0 < p'_{11} < p_{11}$

REPEAT step

If p'_{11} ever reaches 1 then it divides all others, so we can reduce first row and column (except p'_{11}) to zeros

Process must terminate in at most p_{11} iterations

20

Summary

$$\mathbf{P} \xrightarrow[\text{elementary row and column operations}]{(a)} \left[\begin{array}{c|ccc} q_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{P}' & \\ 0 & & (m-1) \times (n-1) & \end{array}\right]$$

$$\mathbf{P}' \xrightarrow[\text{elementary row and column operations}]{(b)} \left[\begin{array}{c|ccc} q_2 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \mathbf{P}'' & \\ 0 & & (m-2) \times (n-2) & \end{array}\right]$$

these operations can be regarded as acting on the whole $m \times n$ matrix without disturbing its first row and column

So:

$$\mathbf{P} \xrightarrow[\text{elementary row and column operations}]{\text{(a) then (b)}} \left[\begin{array}{cc|ccc} q_1 & 0 & 0 & \cdots & 0 \\ 0 & q_2 & 0 & \cdots & 0 \\ \hline 0 & 0 & & & \\ \vdots & \vdots & & \mathbf{P}'' & \\ 0 & 0 & & (m-2) \times (n-2) & \end{array}\right]$$

And so on …
… until finished or until stage in Frame 15 or Frame 18
Then reduce final row or column

We summarize the major result from the tape as follows.

Theorem 3.1 Decomposition of finitely presented Abelian groups

If A is a finitely presented Abelian group with presentation

$$A = \langle a_1, \ldots, a_n : w_1 = 0, \ \ldots, \ w_m = 0 \rangle,$$

then A can be written as a direct product

$$\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n},$$

where

$$q_i \geq 0, \quad i = 1, \ldots, n.$$

Terms $\mathbb{Z}_1$ are trivial and may be omitted; terms $\mathbb{Z}_0$ are usually written in the more familiar form $\mathbb{Z}$.

When using the Reduction Algorithm, we have seen how different choices may lead to different diagonal matrices and hence to different direct product decompositions. Where this occurred, our knowledge of cyclic groups and their direct products enabled us to see why the resulting groups are the same. This knowledge also enables us to express a finitely presented Abelian group as a *canonical* direct product of cyclic groups, which is unique.

The result that we shall obtain is the following.

Theorem 3.2 Canonical decomposition of finitely presented Abelian groups

If A is a finitely presented Abelian group with presentation

$$A = \langle a_1, \ldots, a_n : w_1 = 0, \ \ldots, \ w_m = 0 \rangle,$$

then A can be written as a direct product

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n},$$

where

$$d_i \geq 0, \ d_i \mid d_{i+1}, \quad i = 1, \ldots, n-1.$$

The d_is which are greater than one are unique and are called the **torsion coefficients** of A.

The *number* of zeros among the d_is (that is, the number of $\mathbb{Z}$s in the direct product) is also uniquely determined and is called the **rank** of A.

This unique direct product decomposition of A is known as the **canonical decomposition** or **canonical form** of A.

We postpone the proof of the Canonical Decomposition Theorem until Section 4. To complete this section we first illustrate the calculation of torsion coefficients and rank, and then look at a consequence of the theorem.

Example 3.1

Suppose that the Reduction Algorithm has been applied to a finite presentation of a group A to give the decomposition

$$A \cong \mathbb{Z}_6 \times \mathbb{Z}_9 \times \mathbb{Z}_{14} \times \mathbb{Z} \times \mathbb{Z}.$$

Since $6 = 2 \times 3$ and 2 and 3 are coprime, we may write

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Similarly,

$$\mathbb{Z}_{14} \cong \mathbb{Z}_2 \times \mathbb{Z}_7.$$

We cannot decompose $\mathbb{Z}_9$ in the same way since the only factorization of 9 into coprime factors is $9 = 1 \times 9$. The corresponding direct product is $\mathbb{Z}_1 \times \mathbb{Z}_9$ and we may omit the trivial term $\mathbb{Z}_1$.

Hence, decomposing the finite cyclic groups into cyclic groups of coprime order, where possible, gives

$$\begin{aligned} A &\cong (\mathbb{Z}_2 \times \mathbb{Z}_3) \times \mathbb{Z}_9 \times (\mathbb{Z}_2 \times \mathbb{Z}_7) \times \mathbb{Z} \times \mathbb{Z} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_7 \times \mathbb{Z} \times \mathbb{Z}. \end{aligned}$$

Because of the required divisibility property, and the fact that the torsion coefficients are positive, the last torsion coefficient must be the largest. Since it is divisible by all the others, it must contain the highest available power of all possible prime factors. Hence, this last torsion coefficient must be $2 \times 9 \times 7 = 126$. At this stage we have

The required divisibility property also means that the $\mathbb{Z}$s in the direct product must come last, after the finite terms, since $\mathbb{Z} = \mathbb{Z}_0$ and since we know that every integer divides zero and the only integer divisible by zero is zero itself.

$$\begin{aligned} A &\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_7) \times \mathbb{Z} \times \mathbb{Z} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{126} \times \mathbb{Z} \times \mathbb{Z}. \end{aligned}$$

Next, from the remaining terms $\mathbb{Z}_2 \times \mathbb{Z}_3$ we again pick out the highest powers of the available primes and combine them. These highest powers are 2 and 3 (using up both $\mathbb{Z}_2$ and $\mathbb{Z}_3$), and, since $2 \times 3 = 6$, we obtain

$$A \cong \mathbb{Z}_6 \times \mathbb{Z}_{126} \times \mathbb{Z} \times \mathbb{Z}.$$

We have now used up all the terms. Hence the torsion coefficients of A are 6 and 126 and the rank of A is 2. ♦

Exercise 3.4

Find the torsion coefficients and the rank of each of the following Abelian groups:

(a) $A = \mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z}$;

(b) $A = \mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{15} \times \mathbb{Z}_{21}$;

(c) $A = \mathbb{Z}_p \times \mathbb{Z}_{p^2q} \times \mathbb{Z}_{pq} \times \mathbb{Z}_{pq^3}$, where p and q are distinct primes.

There is a useful consequence of the Canonical Decomposition Theorem. It provides an algorithm for deciding whether or not two finitely presented Abelian groups are isomorphic.

Because of the uniqueness in the Canonical Decomposition Theorem, if we express two groups in canonical form, they are isomorphic if, and only if, the canonical decompositions (after omitting any trivial $\mathbb{Z}_1$ terms) are the same.

Exercise 3.5

Let A and B be Abelian groups of order 600 defined by

$$\begin{aligned} A &= \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{15}, \\ B &= \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_5 \times \mathbb{Z}_{10}. \end{aligned}$$

Determine whether or not A and B are isomorphic.

Exercise 3.6

Let C and D be Abelian groups defined by

$$\begin{aligned} C &= \langle a, b, c, d \colon\ 2a = 0,\ 3b = 0 \rangle, \\ D &= \langle a, b, c \colon\ 6a = 0 \rangle. \end{aligned}$$

Determine whether or not C and D are isomorphic.

4 EXISTENCE AND UNIQUENESS OF TORSION COEFFICIENTS AND RANK

We begin this section by proving the *existence* part of the Canonical Decomposition Theorem. That is to say, if A is a finitely presented Abelian group with presentation

$$A = \langle a_1, \dots, a_n : \, w_1 = 0, \, \dots, \, w_m = 0 \rangle,$$

then A can be written as a direct product

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$$

with

$$d_i \geq 0, \quad d_i \mid d_{i+1}, i = 1, \dots, n-1.$$

We know that, by applying the Reduction Algorithm, we can express A as a direct product

$$\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_n}, \quad q_i \geq 0, \, i = 1, \dots, n.$$

For each q_i which is greater than 1, we write it as a product of powers of distinct primes. Since each of these prime powers is coprime to all the others, the cyclic group $\mathbb{Z}_{q_i}$ may be written as a direct product of cyclic groups whose orders are powers of distinct primes. Having done this for all appropriate q_is, we recombine the cyclic groups as follows to produce $\mathbb{Z}_{d_i}$s with the d_is having the required divisibility properties.

To begin with we put all $\mathbb{Z}_1$s at the beginning and all $\mathbb{Z}_0$s at the end.

For each prime appearing we take the highest power available. The last positive d_i is the product of these. The corresponding group is the product of the cyclic groups which, because of the coprime orders, is the cyclic group $\mathbb{Z}_{d_i}$.

We have chosen a rather wordy and descriptive proof in order to avoid a symbolic notation for the prime decomposition of each q_i. Such notation would inevitably involve clumsy expressions of the form

$$q_i = p_{i1}^{\alpha_{i1}} \dots p_{il_i}^{\alpha_{il_i}}.$$

The descriptive proof corresponds exactly to the method used in the solutions to Exercises 3.4 and 3.5.

Now consider the remaining cyclic groups of prime power order. Once again, for each remaining prime, we take the highest power available. The penultimate positive d_i is the product of these prime powers, and the corresponding cyclic group $\mathbb{Z}_{d_i}$ is the direct product of the corresponding individual cyclic groups.

We continue in this way until all the cyclic groups of prime power order have been used.

The divisibility property must hold for the d_is created, for the following reason. Any prime p occurring in d_i must occur in d_{i+1} to the same or higher power. Hence d_i divides d_{i+1}. We have already arranged that the 1s appear at the beginning and so divide all subsequent d_is. We have also arranged that the 0s are at the end and hence are divisible by all preceding d_is.

This completes the existence proof.

Now we turn to the *uniqueness* of the torsion coefficients and the rank.

To be quite specific, we shall show that a finitely presented Abelian group A has a unique decomposition

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n},$$

where n is the number of generators and d_i divides d_{i+1} for $i = 1, \dots, n-1$.

Some of the first d_is may be 1s, and the resulting $\mathbb{Z}_{d_i}$ are trivial and may be omitted, as may the 1s from the list of torsion coefficients. Some of the last d_is may be zeros, and the resulting $\mathbb{Z}_{d_i}$s are $\mathbb{Z}$s (the number of zeros is the rank).

The precise statement of the theorem we shall prove is as follows.

Theorem 4.1

Let A be an Abelian group such that

$$\begin{aligned} A &\cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n} \\ &\cong \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_m}, \end{aligned}$$

where each d_i and e_i is either 0 or greater than 1 and where d_i divides d_{i+1} for $i = 1, \ldots, n-1$ and e_i divides e_{i+1} for $i = 1, \ldots, m-1$. Then

$$n = m \quad \text{and} \quad d_i = e_i,\ i = 1, \ldots, n.$$

Our overall proof strategy uses the Principle of Mathematical Induction on the minimum of n and m.

The proof will require some preliminary results, which we ask you to obtain in the following exercises.

Exercise 4.1

(a) Prove that, if d_1 and d_2 are integers greater than 1 with d_1 dividing d_2, then

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$$

is not cyclic.

(b) Prove that, if $d > 1$ is an integer, then

$$\mathbb{Z}_d \times \mathbb{Z}$$

is not cyclic.

(c) Prove that $\mathbb{Z} \times \mathbb{Z}$ is not cyclic.

Exercise 4.2

Let H and K be subgroups of the Abelian group A such that A is the internal direct product of H and K. Show that

$$A/K \cong H.$$

Hint Use the Internal Direct Product Theorem, then define an appropriate function $\phi : A \to H$ and use the First Isomorphism Theorem (from *Unit IB4*).

Exercise 4.3

Let A be a non-trivial finitely presented Abelian group.

(a) Show that A has non-identity elements of finite order if and only if A has torsion coefficients.

(b) If A has non-identity elements of finite order, show that the largest such order is equal to the largest torsion coefficient.

The results of Exercise 4.1 establish that an Abelian group with two (or more) non-trivial terms in its canonical decomposition cannot be cyclic. This follows from the exercise because the product of these non-trivial terms is of one of the forms described in Exercise 4.1. The subgroup corresponding to these terms is not cyclic and so cannot be the subgroup of a cyclic group.

The non-trivial terms are those other than the $\mathbb{Z}_1$s.

The result of Exercise 4.3 shows that there is a torsion coefficient if and only if the group contains non-identity elements of finite order. If this is the case then the largest such finite order is uniquely determined and is the largest torsion coefficient.

We are now in a position to put together a proof of our theorem.

Proof of Theorem 4.1

As indicated earlier, we use the Principle of Mathematical Induction on the minimum of n and m.

If the minimum is 1, we may assume that $n = 1$ and that

$$A \cong \mathbb{Z}_{d_1} \cong \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_m}.$$

Thus A is cyclic and, by the the remarks made above, there can be only one non-trivial term on the right-hand side. Hence $m = 1$ and $d_1 = e_1$.
Thus the result is true when the minimum is 1.

Now assume that the result is true if the minimum is $k \geq 1$ and consider the case where the minimum is $k + 1 \geq 2$. We may assume that $n = k + 1$. We consider

$$\begin{aligned} A &\cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_{k+1}} \\ &\cong \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_l}, \end{aligned}$$

where d_i divides d_{i+1} for $i = 1, \ldots, k$ and e_i divides e_{i+1} for $i = 1, \ldots, l - 1$ and where $l \geq k + 1$.
We consider two cases according to whether A has or has not got non-identity elements of finite order.

If A has no non-identity elements of finite order then, by the result of Exercise 4.3, all the d_is and e_is are zero. It only remains to prove that there are the same number of d_is as e_is.
Since we have $\mathbb{Z}_{d_1} = \mathbb{Z}_{e_1} = \mathbb{Z}$, taking quotients and applying the result from Exercise 4.2, we obtain

$$\begin{aligned} A/\mathbb{Z} &\cong \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_{k+1}} \\ &\cong \mathbb{Z}_{e_2} \times \cdots \times \mathbb{Z}_{e_l}. \end{aligned}$$

There are k terms in the first of these direct products and so, by the inductive hypothesis, the two products must have the same number of terms. Hence $k = l - 1$, and so $k + 1 = l$ as required.

If A has non-identity elements of finite order then, by the result of Exercise 4.3, the largest torsion coefficient, d say, of A is uniquely determined. Hence each of the decompositions for A has a term $\mathbb{Z}_d$. Again we take quotients, this time by $\mathbb{Z}_d$.
The two quotients are isomorphic to direct products of all the terms in the original expressions for A except the term $\mathbb{Z}_d$. Since the first of these quotients contains at most k terms, by the inductive hypothesis the two isomorphic expressions for $A/\mathbb{Z}_d$ are identical, and hence so are the original expressions for A. ■

5 FINITELY GENERATED ABELIAN GROUPS

In this section we shall show that the result of the Canonical Decomposition Theorem still holds if we assume only that the Abelian group is finitely generated rather than finitely presented. That is, we remove the restriction that there be only a finite number of relations. The proof involves quite a number of steps, but the individual steps involve only techniques that you have seen before.

In Section 1 we defined what is meant by the Abelian group given by a finite presentation. For the presentation

$$A = \langle a_1, \ldots, a_n : \, w_1 = 0, \, \ldots, \, w_m = 0 \rangle$$

the group was defined to be the quotient

$$A = \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n \text{ copies}} / K,$$

where K is the smallest (normal) subgroup of

$$\overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n \text{ copies}}$$

containing the elements corresponding to the words $w_1, \ldots, w_m$.

The Reduction Algorithm in Sections 2 and 3 enables us to write the group as a direct product of cyclic groups which, after some manipulation, can be written in the canonical form

Theorem 3.2.

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n},$$

where

$$d_i \in \mathbb{Z}, \quad d_i \geq 0, \quad d_i \mid d_{i+1}, \; i = 1, \ldots, n-1.$$

We now turn our attention to Abelian groups which we know to be finitely generated but for which we are not necessarily given a finite presentation. Thus we know that the Abelian group A is such that

$$A = \langle a_1, \ldots, a_n \rangle.$$

Taking our cue from Section 1, we consider the homomorphism ϕ from the free Abelian group on n generators to A,

$$\phi : \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n \text{ copies}} \to A,$$

defined by

$$\phi((\alpha_1, \ldots, \alpha_n)) = \alpha_1 a_1 + \cdots + \alpha_n a_n.$$

In A the generators $a_1, \ldots, a_n$ will satisfy a (possibly infinite) set of relations. If these are written in standard form, each will correspond to an element of the free Abelian group.

Suppose that such a relation is

$$\alpha_1 a_1 + \cdots + \alpha_n a_n = e.$$

The corresponding element of the free Abelian group is

$$w = (\alpha_1, \ldots, \alpha_n).$$

Hence, by the definition of ϕ, we know that $\phi(w) = e$. That is, the element of the free Abelian group corresponding to a relation is in the kernel of ϕ.

Conversely, if $(\beta_1, \ldots, \beta_n)$ is in the kernel of ϕ, then

$$\begin{aligned} \phi((\beta_1, \ldots, \beta_n)) &= \beta_1 a_1 + \cdots + \beta_n a_n \\ &= e. \end{aligned}$$

Thus every element of the kernel corresponds to a relation (in standard form) satisfied by the generators.

So the kernel of ϕ corresponds to the set of all possible relations (in standard form) between the generators of A.

Since the a_is generate A, the homomorphism ϕ is *onto* and so, by the First Isomorphism Theorem,

$$A \cong \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{n \text{ copies}} / \operatorname{Ker}(\phi).$$

We can sum up the above discussion by saying that the phrases 'finitely generated Abelian group with n generators' and 'quotient of the free Abelian group on n generators' mean the same thing.

We now turn to the extension of the Canonical Decomposition Theorem to finitely generated Abelian groups, whether or not we are given a finite presentation.

Now, for an infinite number of relations, we cannot write down the corresponding matrix. Hence the proof of the Canonical Decomposition Theorem for finitely presented Abelian groups, which relied on the Reduction Algorithm, is not valid for finitely generated Abelian groups. Therefore, in order to prove the Canonical Decomposition Theorem for finitely generated Abelian groups we shall need a different approach.

The formal statement of the theorem that we shall prove is as follows.

Theorem 5.1 Canonical decomposition of finitely generated Abelian groups

If A is a non-trivial Abelian group generated by a finite number of elements then

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k},$$

where

$$d_i \in \mathbb{Z}, \quad d_i > 1 \text{ or } d_i = 0, \quad d_i \mid d_{i+1}, \ i = 1, \ldots, k-1.$$

The trivial Abelian group, $\{0\}$, is the trivial cyclic group $\mathbb{Z}_1$.

We have avoided d_i values of 1 to remove trivial terms $\mathbb{Z}_1 = \{0\}$ from the direct product.

From the form of A, it is generated by a set of k elements which, because we have avoided trivial terms, is in some sense minimal. We shall use this fact in our proof.

In Section 4 the proof of the uniqueness of torsion coefficients and rank was based on the Principle of Mathematical Induction and relied on elements of largest finite order. Our proof here is again based on the Principle of Mathematical Induction but this time looks for (non-identity) generators of smallest finite order.

Exercise 5.1

The Abelian group A is defined by

$$A = \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k},$$
$$d_i \in \mathbb{Z}, \quad d_i > 1 \text{ or } d_i = 0, \quad d_i \mid d_{i+1}, \ i = 1, \ldots, k-1,$$

and has a non-zero element of finite order. Show that, of the generators

$$(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), \ldots, (0, \ldots, 0, 1),$$

the one with smallest order is $(1, 0, \ldots, 0)$, which has order d_1.

With these preliminaries over let us state our strategy. We shall prove the result by use of the Principle of Mathematical Induction on the minimum number of generators of the group. Of all sets of generators containing this minimum number of elements, which we shall refer to a 'minimum set of generators', we shall look for one containing a generator of smallest order.

Before we begin the proof, we need to be absolutely sure of what we mean by a 'minimum set of generators'. The following example illustrates two possible interpretations.

Example 5.1

We have previously seen that

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6.$$

Viewed as this direct product, $\mathbb{Z}_6$ has a set of generators

$$\{(1,0),(0,1)\}.$$

Neither generator is redundant, because discarding either no longer gives the whole group. Hence, in the sense that no proper subset will generate the whole group,

$$\{(1,0),(0,1)\}.$$

is a minimum set of generators for $\mathbb{Z}_6$.

On the other hand, because $\mathbb{Z}_6$ is cyclic, it is generated by one element (for example, $(1,1)$). Therefore, in this sense, $\{(1,1)\}$ is a minimum set of generators. ♦

Throughout the proof, we shall be concerned with the minimum *number* of generators for an Abelian group. In other words, we shall only be concerned with 'minimum sets of generators' in the second sense illustrated in Example 5.1. Therefore, by a 'minimum set of generators' or 'minimum generating set' we shall mean a set of generators containing the minimum possible number of generators.

Proof of Theorem 5.1

To start the induction process, we consider Abelian groups A which possess a minimum generating set containing just one element. In this case the group is cyclic, i.e.

$$A \cong \mathbb{Z}_{d_1}.$$

Since there is only one d_i, the divisibility property is automatically satisfied. Thus the result is true for all Abelian groups with a minimum generating set containing one element.

Now assume the result is true for all Abelian groups with a minimum generating set containing at most $k-1$ generators. Let A be an Abelian group generated by k elements but not fewer (if it were generated by fewer then, by the induction hypothesis, it could already be written in the required form). We shall show that A has a decomposition of the correct form.

Consider the set S of all coefficients occurring in all non-trivial relations on all sets of k generators.

If there are no such relations, i.e. S is the empty set, then the kernel of the homomorphism ϕ defined above by

$$\phi : \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{k \text{ copies}} \to A$$
$$(\alpha_1, \ldots, \alpha_k) \mapsto \alpha_1 a_1 + \cdots + \alpha_k a_k$$

is trivial. Thus, by the First Isomorphism Theorem,

$$A \cong \overbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}^{k \text{ copies}} = \overbrace{\mathbb{Z}_0 \times \cdots \times \mathbb{Z}_0}^{k \text{ copies}},$$

which is of the correct form.

We next observe that, if S is not empty, there is a non-trivial relation and so S contains non-zero elements. It follows that S contains positive elements since, if

$$n_1a_1 + \cdots + n_ka_k = 0$$

is a relation on a minimum set of k generators $a_1, \ldots, a_k$ of A, then so is

$$(-n_1)a_1 + (-n_2)a_2 + \cdots + (-n_k)a_k = 0.$$

This step in the argument corresponds to changing the sign of a row in the Reduction Algorithm.

We now pick the smallest positive element d of S. Thus d appears in some relation involving some possible set of k generators. We can label these generators in such a way that this relation is

$$d_1a_1 + n_2a_2 + \cdots + n_ka_k = 0,$$

where $d_1 = d$, the least positive element of S.

Labelling generators corresponds to interchanging columns in the Reduction Algorithm.

Just to reiterate: k is the smallest possible number of generators for A and $d_1 = d$ is the smallest positive coefficient occurring in *all* relations between *all* possible sets of k generators.

In the next exercises we ask you to show that d_1 divides n_2. □

The minimum order l of a generator a cannot be less than d, since otherwise there would be a relation $la = 0$, where $0 < l < d$, contradicting the definition of d. We shall show later that there is a generator having order $d = d_1$.

Exercise 5.2

Using the Quotient–remainder Theorem, we have

$$n_2 = d_1q + r, \quad 0 \leq r < d_1, \quad q, r \in \mathbb{Z}.$$

Let

$$b_1 = a_1 + qa_2.$$

Here we are changing the generators of A, which corresponds to column operations in the Reduction Algorithm.

Verify that

$$\{b_1, a_2, \ldots, a_k\} \subseteq \langle a_1, a_2, \ldots, a_k\rangle$$

and that

$$\{a_1, a_2, \ldots, a_k\} \subseteq \langle b_1, a_2, \ldots, a_k\rangle.$$

Hence show that

$$A = \langle b_1, a_2, \ldots, a_k\rangle,$$

so that $\{b_1, a_2, \ldots, a_k\}$ is also a minimum set of k generators for A.

Exercise 5.3

By considering the definition of d_1, verify that $r = 0$ and hence that d_1 divides n_2.

Proof of of Theorem 5.1 continued

Exercises 5.2 and 5.3 have shown that d_1 divides n_2. In exactly the same way as in those exercises, we establish that d_1 divides n_i for $i = 3, \ldots, k$.

We now set $n_i = d_1q_i$ for $i = 2, \ldots, k$, and define

$$c_1 = a_1 + q_2a_2 + \cdots + q_ka_k.$$

In fact, q_2 is what we previously called q, in Exercise 5.2.

Consider the elements

$$c_1, a_2, \ldots, a_k.$$

Because all these elements are integer combinations of the a_is, we have

$$\langle c_1, a_2, \ldots, a_k\rangle \subseteq \langle a_1, \ldots, a_k\rangle = A.$$

On the other hand,

$$a_1 = c_1 - q_2a_2 - \cdots - q_ka_k,$$

and so

$$a_1 \in \langle c_1, a_2, \ldots, a_k \rangle.$$

Hence

$$A = \langle a_1, \ldots, a_k \rangle \subseteq \langle c_1, a_2, \ldots, a_k \rangle.$$

Thus

$$A = \langle c_1, a_2, \ldots, a_k \rangle,$$

and we have constructed another new minimum set of k generators for A.

The relation

$$d_1a_1 + n_2a_2 + \cdots + n_ka_k = 0$$

becomes

$$d_1a_1 + d_1q_2a_2 + \cdots + d_1q_ka_k = 0,$$

or, equivalently,

$$d_1(a_1 + q_2a_2 + \cdots + q_ka_k) = 0.$$

In other words

$$d_1c_1 = 0.$$

Furthermore, the fact that d_1 is the smallest positive coefficient in relations between minimum sets of generators means that no relation $lc_1 = 0$ exists for $0 < l < d_1$. So the order of the element c_1 is d_1. Hence

$$\langle c_1 \rangle \cong \mathbb{Z}_{d_1}.$$

Now

$$\langle c_1 \rangle \cap \langle a_2, \ldots, a_k \rangle = \{0\}$$

because, if $a \neq 0$ and

$$a \in \langle c_1 \rangle \cap \langle a_2, \ldots, a_k \rangle,$$

then

$$a = x_1c_1 = x_2a_2 + \cdots + x_ka_k, \quad 0 < x_1 < d_1.$$

This leads to

$$x_1c_1 + (-x_2)a_2 + \cdots + (-x_k)a_k = 0,$$

which contradicts the minimality of d_1. Hence the subgroups

$$\langle c_1 \rangle \quad \text{and} \quad \langle a_2, \ldots, a_k \rangle$$

have trivial intersection.

Furthermore, because $c_1, a_2, \ldots, a_k$ generate A, every element of A is a sum of elements, one from $\langle c_1 \rangle$ and one from $\langle a_2, \ldots, a_k \rangle$. Therefore, since these subgroups have trivial intersection, we can use the Internal Direct Product Theorem to express A as their internal direct product

$$\begin{aligned} A &\cong \langle c_1 \rangle \times \langle a_2, \ldots, a_k \rangle \\ &\cong \mathbb{Z}_{d_1} \times A_1, \end{aligned}$$

where A_1 is generated by $k-1$ generators $a_2, \ldots, a_k$.

Since A_1 has a set of $k-1$ generators, it has a minimum generating set with *at most* $k-1$ elements. So, by the induction hypothesis, A_1 can be written in the form

$$A_1 \cong \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k},$$
$$d_i \in \mathbb{Z}, \quad d_i > 1 \text{ or } d_i = 0, \quad d_i \mid d_{i+1},\ i = 2, \ldots, k-1.$$

It follows that A is a direct product of the correct type, namely

$$A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k}.$$

All that remains to be proved is that d_1 divides d_2.

We have constructed a generator c_1 of $\mathbb{Z}_{d_1}$. Let c_i generate $\mathbb{Z}_{d_i}$ for $i = 2, \ldots, k$. Since d_i is either the order of the cyclic group $\mathbb{Z}_{d_i}$ or 0, we have

$$d_i c_i = 0, \quad i = 1, \ldots, k.$$

Adding these gives the relation

$$d_1 c_1 + \cdots + d_k c_k = 0.$$

It follows from the definition of d_1 and from Exercises 5.2 and 5.3 that d_1 divides d_2, and the proof is complete. ■

The proof that we have just completed not only shows that every finitely generated Abelian group possesses a canonical decomposition but also that it possesses a finite presentation. The elements $c_1, \ldots, c_k$ above are a finite set of generators for A and the corresponding relations giving a finite presentation are

$$d_1 c_1 = 0, \ldots, d_k c_k = 0.$$

Some of these relations may be trivial.

The question remains as to whether *every* Abelian group has a canonical decomposition as a direct product of a *finite* number of cyclic groups. If this were the case then every Abelian group would have a finite set of generators (the set of c_is in the proof above). In the following exercise we ask you to show that this is not the case.

Exercise 5.4

Let A be the Abelian group $(\mathbb{Q}, +)$.

As usual, $\mathbb{Q}$ denotes the rational numbers.

(a) Show that the set

$$\{\tfrac{1}{2}, \tfrac{1}{3}\}$$

does not generate A.

(b) Let r and s be any two elements of A. Show that the set

$$\{r, s\}$$

does not generate A.

Hint Consider the denominators of all elements in the group $\langle r, s \rangle$, and use the fact that there are infinitely many prime numbers.

(c) Show that A has no finite set of generators.

Exercise 5.4 shows that $(\mathbb{Q}, +)$ is not finitely generated and so cannot have a canonical decomposition of the form we have been considering.

We have not settled the question of whether $(\mathbb{Q}, +)$ has a decomposition as a direct product of an *infinite* number of cyclic groups. Discussion of infinite direct products is beyond the scope of this course.

SOLUTIONS TO THE EXERCISES

Solution 1.1

We make use of the 'free' property. From

$$s_1x_1 + \cdots + s_nx_n = t_1x_1 + \cdots + t_nx_n$$

we have

$$(s_1 - t_1)x_1 + \cdots + (s_n - t_n)x_n = 0.$$

It follows that

$$s_1 - t_1 = 0, \ldots, s_n - t_n = 0$$

and the result follows.

Solution 1.2

Since $(1, 0)$ corresponds to x_1, the element corresponding to $2x_1$ is $2 \times (1, 0) = (2, 0)$.
Similarly, the element corresponding to $3x_2$ is $3 \times (0, 1) = (0, 3)$.

Solution 1.3

The subgroup K must contain the elements corresponding to $2x_1$ and $3x_2$. Hence K is the smallest subgroup of $\mathbb{Z} \times \mathbb{Z}$ containing $(2, 0)$ and $(0, 3)$.

Hence K must contain all elements of the form

$$k \times (2, 0) = (2k, 0), \quad k \in \mathbb{Z},$$

and all elements of the form

$$l \times (0, 3) = (0, 3l), \quad l \in \mathbb{Z}.$$

Therefore K must contain all sums

$$(2k, 0) + (0, 3l) = (2k, 3l).$$

However, the set

$$\{(2k, 3l) : \ k, l \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z} \times \mathbb{Z}$ since

$$(2k_1, 3l_1) + (2k_2, 3l_2) = (2(k_1 + k_2), 3(l_1 + l_2)),$$

giving closure,

$$(0, 0) = (2 \times 0, 3 \times 0),$$

giving the identity, and

$$-(2k, 3l) = (2(-k), 3(-l)),$$

giving inverses.

Thus K must contain at least the specified set of elements and, since that set is a subgroup, it must be K, by the minimality of K. This completes the proof.

Solution 1.4

The matrices are as follows:

(a) $\begin{bmatrix} 3 & 2 & 0 \\ 0 & 2 & -5 \\ 6 & 0 & -3 \end{bmatrix}$;

(b) $\begin{bmatrix} 4 & -2 & 0 \\ 6 & 0 & -3 \end{bmatrix}$;

(c) $\begin{bmatrix} 3 & 2 \\ 2 & -5 \\ 6 & -3 \end{bmatrix}$.

Solution 1.5

(a) The matrix is

$$\begin{bmatrix} 2 & 0 \\ 0 & 7 \end{bmatrix}$$

and hence

$$A \cong \mathbb{Z}_2 \times \mathbb{Z}_7.$$

(b) The matrix is

$$\begin{bmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 5 \end{bmatrix}$$

and hence

$$A \cong \mathbb{Z}_4 \times \mathbb{Z}_6 \times \mathbb{Z}_5.$$

Solution 1.6

(a) The matrix has three columns and so the presentation has three generators. The presentation is

$$A = \langle a, b, c\colon\ 5a = 0,\ 7b = 0,\ 0c = 0\rangle.$$

The third relation places no restriction on the generator c and so the corresponding component is $\mathbb{Z}$.
These relations give

$$A \cong \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}.$$

(b) The matrix has three columns and so the presentation has three generators. The presentation is

$$A = \langle a, b, c\colon\ 1a = 0,\ 2b = 0,\ 3c = 0\rangle.$$

These relations give

$$A \cong \mathbb{Z}_1 \times \mathbb{Z}_2 \times \mathbb{Z}_3.$$

We can simplify this direct product by observing that $1\mathbb{Z} = \mathbb{Z}$. Hence $1\mathbb{Z}$ has only one coset in $\mathbb{Z}$ and so the quotient group

$$\mathbb{Z}_1 = \mathbb{Z}/1\mathbb{Z}$$

has only one element. Thus, $\mathbb{Z}_1$ is the trivial group, and we may omit it from the direct product. Hence

$$A \cong \mathbb{Z}_2 \times \mathbb{Z}_3.$$

What we have discovered is that this group has an alternative presentation with only two generators:

$$A = \langle b, c\colon\ 2b = 0,\ 3c = 0\rangle.$$

With diagonal matrices, 'surplus' generators make themselves apparent by the presence of 1s on the diagonal.

(c) The matrix has four columns and so the presentation has four generators. The presentation is

$$A = \langle a, b, c, d\colon\ 2a = 0,\ -5b = 0,\ 7c = 0\rangle.$$

The second relation can be replaced by $5b = 0$, giving a component $\mathbb{Z}_5$. Since there is no relation involving the generator d, the fourth component is $\mathbb{Z}$.
Hence

$$A \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \times \mathbb{Z}.$$

(d) The matrix has three columns and so the presentation has three generators. The presentation is

$$A = \langle a, b, c\colon\ -3a = 0,\ 11b = 0,\ -13c = 0,\ 0a + 0b + 0c = 0\rangle.$$

Replacing each negative integer by its modulus and ignoring the last relation (which contributes nothing), we have

$$A \cong \mathbb{Z}_3 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}.$$

Solution 2.1

Since we have in Example 2.1 reduced the matrix of the relations to the diagonal form

$$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix},$$

we can say that $A \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.

Solution 2.2

The group represented by the matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}$$

is

$$\mathbb{Z}_1 \times \mathbb{Z}_6.$$

As we observed in the solution to Exercise 1.6(b), the group $\mathbb{Z}_1$ is the trivial group and so we can omit it from the direct product. Thus the group above is $\mathbb{Z}_6$.

The group represented by the matrix

$$\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$$

is

$$\mathbb{Z}_2 \times \mathbb{Z}_3.$$

Since 2 and 3 are coprime, we have, by Lemma 5.1 of *Unit GR2*,

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6.$$

Hence, the groups represented by the two different diagonal matrices are the same (up to isomorphism).

Solution 2.3

Since the matrix corresponding to the relations in A has been reduced, in Example 2.3, to the diagonal form

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 15 & 0 \\ 0 & 0 & 60 \end{bmatrix},$$

we have

$$A \cong \mathbb{Z}_2 \times \mathbb{Z}_{15} \times \mathbb{Z}_{60}.$$

Solution 2.4

(a) From now on we shall not indicate the separate applications of the inner loop to obtain each diagonal element in turn. We pick up the calculations at the point where the choice arose.

The details of your solutions to this and the next exercise may differ from ours, depending on your choice of elementary operation at certain points, but your conclusions should be the same as ours.

$$\begin{bmatrix} 4 & 6 & 0 \\ 10 & 0 & 15 \\ -6 & 6 & 15 \end{bmatrix} \mapsto \begin{bmatrix} 4 & 6 & 0 \\ 2 & -12 & 15 \\ -6 & 6 & 15 \end{bmatrix} \qquad R_2 \to R_2 - 2R_1$$

$$\mapsto \begin{bmatrix} 2 & -12 & 15 \\ 4 & 6 & 0 \\ -6 & 6 & 15 \end{bmatrix} \qquad R_1 \leftrightarrow R_2$$

$$\mapsto \begin{bmatrix} 2 & -12 & 1 \\ 4 & 6 & -28 \\ -6 & 6 & 57 \end{bmatrix} \qquad C_3 \to C_3 - 7C_1$$

You may have made a different choice of elementary operation here.

$$\mapsto \begin{bmatrix} 1 & -12 & 2 \\ -28 & 6 & 4 \\ 57 & 6 & -6 \end{bmatrix} \qquad C_1 \leftrightarrow C_3$$

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ -28 & -330 & 60 \\ 57 & 690 & -120 \end{bmatrix} \qquad C_2 \to C_2 + 12C_1, \quad C_3 \to C_3 - 2C_1$$

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & -330 & 60 \\ 0 & 690 & -120 \end{bmatrix} \qquad R_2 \to R_2 + 28R_1, \quad R_3 \to R_3 - 57R_1$$

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 60 & -330 \\ 0 & -120 & 690 \end{bmatrix} \qquad C_2 \leftrightarrow C_3$$

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 60 & 30 \\ 0 & -120 & -30 \end{bmatrix} \qquad C_3 \to C_3 + 6C_2$$

You may have made a different choice of elementary operation here.

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 30 & 60 \\ 0 & -30 & -120 \end{bmatrix} \qquad C_2 \leftrightarrow C_3$$

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & -30 & -60 \end{bmatrix} \qquad C_3 \to C_3 - 2C_2$$

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & 0 & -60 \end{bmatrix} \qquad R_3 \to R_3 + R_2$$

$$\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & 0 & 60 \end{bmatrix} \qquad C_3 \to -C_3$$

(b) The diagonal matrix

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 30 & 0 \\ 0 & 0 & 60 \end{bmatrix},$$

represents the group

$$\mathbb{Z}_1 \times \mathbb{Z}_{30} \times \mathbb{Z}_{60}.$$

Since $\mathbb{Z}_1$ is the trivial group, we have the group

$$\mathbb{Z}_{30} \times \mathbb{Z}_{60}.$$

(c) The groups obtained from the two diagonal forms are

$$\mathbb{Z}_2 \times \mathbb{Z}_{15} \times \mathbb{Z}_{60} \quad \text{and} \quad \mathbb{Z}_{30} \times \mathbb{Z}_{60}.$$

To show that they are the same (up to isomorphism) we need to show that

$$\mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_{30}.$$

However, this follows from the fact that $30 = 2 \times 15$ and that 2 and 15 are coprime.

Solution 2.5

We have to reduce the matrix

$$\begin{bmatrix} 3 & 2 & 4 \\ 6 & 1 & 7 \\ 2 & 3 & 6 \end{bmatrix}$$

to diagonal form. We shall not write out the operations explicitly.

$$\begin{aligned}
\begin{bmatrix} 3 & 2 & 4 \\ 6 & 1 & 7 \\ 2 & 3 & 6 \end{bmatrix} &\mapsto \begin{bmatrix} 6 & 1 & 7 \\ 3 & 2 & 4 \\ 2 & 3 & 6 \end{bmatrix} \\
&\mapsto \begin{bmatrix} 1 & 6 & 7 \\ 2 & 3 & 4 \\ 3 & 2 & 6 \end{bmatrix} \\
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 2 & -9 & -10 \\ 3 & -16 & -15 \end{bmatrix} \\
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & -9 & -10 \\ 0 & -16 & -15 \end{bmatrix} \\
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 9 & 10 \\ 0 & -16 & -15 \end{bmatrix} \\
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 9 & 1 \\ 0 & -16 & 1 \end{bmatrix}
\end{aligned}$$

You may have made a different choice of elementary operation here.

$$\begin{aligned}
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 9 \\ 0 & 1 & -16 \end{bmatrix} \\
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -25 \end{bmatrix}
\end{aligned}$$

You may have made a different choice of elementary operation here.

$$\begin{aligned}
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -25 \end{bmatrix} \\
&\mapsto \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 25 \end{bmatrix}
\end{aligned}$$

Hence the Abelian group is

$$A \cong \mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_{25} \cong \mathbb{Z}_{25}.$$

Solution 3.4

Using the same technique as in Example 3.1 we obtain the following.

(a)
$$\begin{aligned} A &= \mathbb{Z}_6 \times \mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{15} \times \mathbb{Z} \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_3) \times \mathbb{Z}_8 \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_3 \times \mathbb{Z}_5) \times \mathbb{Z} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times (\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \times \mathbb{Z} \\ &\cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \times \mathbb{Z}_{120} \times \mathbb{Z} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_{30} \times \mathbb{Z}_{120} \times \mathbb{Z}. \end{aligned}$$

Hence, the torsion coefficients of A are 2, 30 and 120 and the rank is 1.

(b)
$$\begin{aligned} A &= \mathbb{Z}_{10} \times \mathbb{Z}_{12} \times \mathbb{Z}_{15} \times \mathbb{Z}_{21} \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_3 \times \mathbb{Z}_4) \times (\mathbb{Z}_3 \times \mathbb{Z}_5) \times (\mathbb{Z}_3 \times \mathbb{Z}_7) \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times (\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7) \\ &\cong \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \times \mathbb{Z}_{420} \\ &\cong \mathbb{Z}_3 \times \mathbb{Z}_{30} \times \mathbb{Z}_{420}. \end{aligned}$$

Hence, the torsion coefficients of A are 3, 30 and 420 and the rank is 0.

(c)
$$\begin{aligned} A &= \mathbb{Z}_p \times \mathbb{Z}_{p^2q} \times \mathbb{Z}_{pq} \times \mathbb{Z}_{pq^3} \\ &\cong \mathbb{Z}_p \times (\mathbb{Z}_{p^2} \times \mathbb{Z}_q) \times (\mathbb{Z}_p \times \mathbb{Z}_q) \times (\mathbb{Z}_p \times \mathbb{Z}_{q^3}) \\ &\cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_{q^3} \\ &\cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q \times (\mathbb{Z}_{p^2} \times \mathbb{Z}_{q^3}) \\ &\cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_q \times \mathbb{Z}_{p^2q^3} \\ &\cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q \times (\mathbb{Z}_p \times \mathbb{Z}_q) \times \mathbb{Z}_{p^2q^3} \\ &\cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_{pq} \times \mathbb{Z}_{p^2q^3} \\ &\cong \mathbb{Z}_p \times (\mathbb{Z}_p \times \mathbb{Z}_q) \times \mathbb{Z}_{pq} \times \mathbb{Z}_{p^2q^3} \\ &\cong \mathbb{Z}_p \times \mathbb{Z}_{pq} \times \mathbb{Z}_{pq} \times \mathbb{Z}_{p^2q^3}. \end{aligned}$$

Hence, the torsion coefficients of A are p, pq, pq and p^2q^3 and the rank is 0.

Solution 3.5

We apply the procedure used above to express each of A and B in canonical form.

$$\begin{aligned} A &= \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{15} \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \times (\mathbb{Z}_3 \times \mathbb{Z}_5) \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ &\cong (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \\ &\cong \mathbb{Z}_{10} \times \mathbb{Z}_{60}. \end{aligned}$$

Thus, A has rank 0 and torsion coefficients 10 and 60.

$$\begin{aligned} B &= \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_5 \times \mathbb{Z}_{10} \\ &\cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3) \times \mathbb{Z}_5 \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \\ &\cong \mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_5) \times (\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5) \\ &\cong \mathbb{Z}_2 \times \mathbb{Z}_{10} \times \mathbb{Z}_{30}. \end{aligned}$$

Thus, B has rank 0 and torsion coefficients 2, 10 and 30.

Hence, A and B are not isomorphic.

Solution 3.6

Firstly, the presentation of C has four generators. We can write down the corresponding matrix as

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

This is in diagonal form, so we can read off the direct product form as

$$C \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z} \times \mathbb{Z}.$$

This is not in canonical form, but can easily be rewritten in canonical form as

$$C \cong \mathbb{Z}_6 \times \mathbb{Z} \times \mathbb{Z}.$$

The group C has rank 2 and the single torsion coefficient 6.

Similarly, the matrix for the presentation of D is

$$\begin{bmatrix} 6 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Hence,

$$D \cong \mathbb{Z}_6 \times \mathbb{Z} \times \mathbb{Z},$$

which is in canonical form.

Hence, C and D are isomorphic.

Solution 4.1

(a) The group $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ has order $d_1 d_2$.

If (x, y) is any element of this direct product, then

$$\begin{aligned} d_2 \times (x, y) &= (d_2 x, d_2 y) \\ &= (0, 0). \end{aligned}$$

The second 0 appears because, by Lagrange's Theorem, the order of y must divide d_2. The first 0 appears because, by Lagrange's Theorem, the order of x is a factor of d_1, which is in turn a factor of d_2.

As $d_2 < d_1 d_2$ (since $d_1 > 1$), no element of the direct product has order $d_1 d_2$, and so the group cannot be cyclic.

(b) There are only two types of cyclic group, finite and infinite. We rule each out in turn.

The group $\mathbb{Z}_d \times \mathbb{Z}$ is infinite (it has a subgroup isomorphic to $\mathbb{Z}$) and so cannot be a finite cyclic group.
It also contains the non-identity element $(1, 0)$, which has finite order d, and so the group $\mathbb{Z}_d \times \mathbb{Z}$ cannot be (isomorphic to) the infinite cyclic group $\mathbb{Z}$.

(c) We show that no element (x, y) of $\mathbb{Z} \times \mathbb{Z}$ can generate the whole group.

The elements generated by (x, y) are of the form (nx, ny), for some integer n. In order to generate the element $(1, 1)$, we must have either $x = y = 1$ or $x = y = -1$. Neither of these possibilities can generate the element $(1, 0)$. This completes the proof.

Solution 4.2

Since A is the internal direct product of H and K, where H and K are subgroups of A, we can use the additive form of the Internal Direct Product Theorem to write any element $a \in A$ *uniquely* as

$$a = h + k, \quad h \in H, k \in K.$$

The theorem tells us that $A = H + K$ where $H \cap K = \{0\}$.

Using the second part of the hint we now define ϕ as follows:

$$\begin{aligned}\phi : A &\to H\\ a &\mapsto h\end{aligned}$$

where $a = h + k$. The fact that h and k are unique means that ϕ is well-defined.

We first verify that ϕ is a homomorphism. Suppose that

$$a = h + k \quad \text{and} \quad a' = h' + k'$$

are elements in A with $h, h' \in H$ and $k, k' \in K$.

By definition,

$$\phi(a) = h \quad \text{and} \quad \phi(a') = h'.$$

Now, since A is Abelian,

$$\begin{aligned}a + a' &= (h + k) + (h' + k')\\ &= (h + h') + (k + k').\end{aligned}$$

Hence, as $h + h' \in H$ and $k + k' \in K$, we have

$$\begin{aligned}\phi(a + a') &= h + h'\\ &= \phi(a) + \phi(a').\end{aligned}$$

This completes the proof that ϕ is a homomorphism.

Next we show that the kernel of ϕ is K.

Suppose that $\phi(a) = 0$ and that $a = h + k$, where $h \in H$ and $k \in K$. From the definition of ϕ, we have $h = 0$, and so $a = k \in K$. This shows that

$$\operatorname{Ker}(\phi) \subseteq K.$$

On the other hand, every element $K = 0 + k \in K$ is mapped to 0, and so

$$K \subseteq \operatorname{Ker}(\phi).$$

This completes the proof that $\operatorname{Ker}(\phi) = K$.

To apply the First Isomorphism Theorem to obtain the desired result, it remains to prove that ϕ is onto. For every element $h \in H$, $A = H + K$ contains the element $h + 0$. So the image of ϕ contains the element

$$\phi(h + 0) = h.$$

This completes the proof that ϕ is onto.

Therefore, by the First Isomorphism Theorem,

$$A/\operatorname{Ker}(\phi) = A/K \cong H.$$

Solution 4.3

(a) If A has a torsion coefficient d, then it has a subgroup isomorphic to $\mathbb{Z}_d$, which is finite. Since, by definition of torsion coefficient, $d > 1$, a generator of $\mathbb{Z}_d$ is a non-identity element of finite order d.

Conversely, if A has no torsion coefficients, then since A is non-trivial it must be isomorphic to a direct product of copies of $\mathbb{Z}$. That is, A is a free Abelian group and so has no non-identity elements of finite order. To see this, take any non-identity element $a \in A$, which has the form

$$a = (z_1, \ldots, z_n),$$

where the z_i are integers, at least one of which is non-zero. Hence, for any positive integer k,

$$ka = (kz_1, \ldots, kz_n) \neq 0.$$

(b) Using the result in part (a), the information that we are given about A means that we can write A in canonical form as

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

Let a be any element of finite order in A. Then a can be written as

$$a = (z_1, \ldots, z_k, z_{k+1}, \ldots, z_n),$$

where $z_i \in \mathbb{Z}_{d_i}$ for $i = 1, \ldots, k$ and $z_i \in \mathbb{Z}$ for $i = k + 1, \ldots, n$.
Since a has finite order, we have

$$z_{k+1} = \cdots = z_n = 0.$$

Now consider

$$\begin{aligned} d_k a &= d_k \times (z_1, \ldots, z_k, 0, \ldots, 0) \\ &= (d_k z_1, \ldots, d_k z_k, 0, \ldots, 0) \\ &= (0, \ldots, 0, 0, \ldots, 0). \end{aligned}$$

Hence the order of a divides d_k and therefore cannot exceed d_k. So, the largest possible such order is d_k.

The reason that all the components are 0 is as follows. For each d_i with $i \leq k$, we have d_i divides d_k. Since $d_i z_i = 0$ in $\mathbb{Z}_{d_i}$, it follows that $d_k z_i = 0$.

On the other hand, A contains a generator for its cyclic subgroup $\mathbb{Z}_{d_k}$ which has order d_k. So the largest possible order, d_k, is achieved.

Solution 5.1

Since A has a non-zero element of finite order, not all of the d_is can be 0.

By the divisibility property, $d_1 \neq 0$. As 1 is a generator of $\mathbb{Z}_{d_1}$, it follows that

$$(1, 0, 0, \ldots, 0) \in \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$$

has order d_1.
Similarly the ith generator has order d_i if $d_i > 1$, and infinite order if $d_i = 0$.

By the divisibility property, if d_j is the last of the non-zero d_is, $d_1 \leq d_2 \leq \cdots \leq d_j$, and so $(1, 0, \ldots, 0)$ is the generator of smallest order.

Solution 5.2

Since $b_1 = a_1 + qa_2$, it follows that

$$b_1 \in \langle a_1, a_2, \ldots, a_k \rangle$$

and, hence,

$$\{b_1, a_2, \ldots, a_k\} \subseteq \langle a_1, a_2, \ldots, a_k \rangle.$$

Conversely, as $a_1 = b_1 - qa_2$,

$$a_1 \in \langle b_1, a_2, \ldots, a_k \rangle$$

and, hence,

$$\{a_1, a_2, \ldots, a_k\} \subseteq \langle b_1, a_2, \ldots, a_k \rangle.$$

Thus

$$\langle b_1, a_2, \ldots, a_k \rangle \subseteq \langle a_1, a_2, \ldots, a_k \rangle$$
$$\langle a_1, a_2, \ldots, a_k \rangle \subseteq \langle b_1, a_2, \ldots, a_k \rangle$$

and the result follows.

Solution 5.3

The solution to the previous exercise gives us a new minimum set of k generators

$$\{b_1, a_2, \ldots, a_k\}.$$

The relation

$$d_1a_1 + n_2a_2 + \cdots + n_ka_k = 0$$

can be rewritten as

$$d_1a_1 + (d_1q + r)a_2 + \cdots + n_ka_k = 0.$$

This is

$$d_1(a_1 + qa_2) + ra_2 + \cdots + n_ka_k = 0,$$

or, equivalently,

$$d_1b_1 + ra_2 + \cdots + n_ka_k = 0.$$

This is a relation on a minimum set of k generators and we also have

$$0 \leq r < d_1.$$

By the minimality of d_1, we have $r = 0$ and so

$$d_1 \mid n_2.$$

Solution 5.4

(a) The elements generated by $\frac{1}{2}$ and $\frac{1}{3}$, i.e. the elements of the subgroup $\langle \frac{1}{2}, \frac{1}{3} \rangle$, are of the form

$$m \times \tfrac{1}{2} + n \times \tfrac{1}{3} = \frac{3m + 2n}{6}, \quad m, n \in \mathbb{Z}.$$

Clearly this subgroup contains only rational numbers with denominators 1, 2, 3 or 6. It does not contain $\frac{1}{5}$, for example, and so is not the whole of A.

(b) Let $r = a/b$ and $s = c/d$ with $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$. Any element of $\langle r, s\rangle$ is of the form

$$m \times \frac{a}{b} + n \times \frac{c}{d} = \frac{dam + bcn}{bd}, \quad m, n \in \mathbb{Z}.$$

If p is any prime which does not occur in the factorization of bd, then $1/p$ cannot be of this form and so is not in $\langle r, s\rangle$. Since there is an infinite number of primes, and hence one greater than any positive integer $|bd|$, such a p always exists, and hence no set of two elements can generate A.

(c) Consider any finite set of elements $r_1, \ldots, r_k$ of A. By an argument similar to those above, if p is a prime not occurring in the denominators of the r_is, then $1/p$ is not in $\langle r_1, \ldots, r_k\rangle$. Since there is an infinite number of primes, such a p always exists, and hence no finite set of elements can generate A.

OBJECTIVES

After you have studied this unit, you should be able to:

(a) write down the integer matrix corresponding to a given finite presentation for an Abelian group;

(b) given an integer matrix, write down the corresponding presentation for an Abelian group;

(c) apply the Reduction Algorithm to an integer matrix to reduce it to diagonal form;

(d) write down the direct product of cyclic groups corresponding to an integer matrix in diagonal form;

(e) reduce any direct product of cyclic groups to canonical form;

(f) for a finitely presented Abelian group, find its torsion coefficients and rank;

(g) produce simple proofs using the proof techniques of this unit.

INDEX